JAN 2

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

Helmut Hasse

Band 176

Heft 3

Ausgegeben am 18. Dezember 1936

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

Berlin W 35 und Leipzig

1936

Band 176. Heft 3.

Inhaltsverzeichnis.

	Seite
Witt, Ernst, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n	126
Teichmüller, Oswald, Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper	141
Witt, Ernst, Schiefkörper über diskret bewerteten Körpern	153
Teichmüller, Oswald, Zerfallende zyklische p-Algebren	157
Schmid, Hermann Ludwig, Zur Arithmetik der zyklischen p-Körper	161
Schmid, Hermann Ludwig, und **Ernst Witt,** Unverzweigte abelsche Körper vom Exponenten p^n über einem algebraischen Funktionenkörper der Charakteristik p	168
Hasse, Helmut, Die Gruppe der p^n-primären Zahlen für einen Primteiler $\mathfrak{p}$ von p	174
Hasse, Helmut, und **Hermann Ludwig Schmid,** Über die Ausnahmeklassen bei abstrakten hyperelliptischen Funktionenkörpern	184

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgendeinem Grunde Textänderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 75 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion unter der Adresse:
An die Redaktion des Journals für die reine und angewandte Mathematik
Professor Dr. Helmut Hasse, Göttingen, Mathematisches Institut, Bunsenstr. 3-5.

Druck von Walter de Gruyter & Co., Berlin W 35
Printed in Germany

Die ersten sieben der in diesem Heft zusammengestellten Arbeiten sind in einer Arbeitsgemeinschaft der mathematischen Fachschaftsabteilung Göttingen entstanden, die von Herrn Witt geleitet wurde. In diesen Arbeiten werden folgende Themen behandelt:

Der innere Aufbau der p-adischen Körper, allgemeiner der diskret bewerteten perfekten Körper und die Struktur der endlichen Schiefkörper über ihnen.

Konstruktion aller zyklischen Körper bzw. Algebren vom Grad p^n; die arithmetische Theorie solcher zyklischen Funktionenkörper; Bestimmung der Divisorenklassen der Ordnung p^n (Charakteristik p).

Zusammenhang der Kummerschen Erzeugung der unverzweigten zyklischen diskret bewerteten perfekten Körper vom Grad p^n (Charakteristik 0) mit der Artin-Schreierschen Erzeugung des Restklassenkörpers (Charakteristik p).

Oberflächlich gesehen, scheint es sich hier um ganz verschiedene Gebiete der Algebra zu handeln, sie sind jedoch, angefangen von den p-adischen Körpern bis zu den Divisorenklassen, alle auf derselben Grundlage behandelt worden.

Die achte Arbeit in diesem Heft ist in einem Seminar von Herrn Hasse entstanden.

Zyklische Körper und Algebren der Charakteristik p vom Grad p^n.

Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p.

Von *Ernst Witt* in Göttingen.

Merkwürdig ist der historische Weg bis zu dieser Arbeit: Er nimmt seinen Anfang bei Artins Untersuchungen über die reellen Körper, führt sodann durch ein Gebiet mit Primzahlcharakteristik, nämlich zuerst über die zyklischen Körper der Grade p und p^2 (Artin und Schreier), dann weiter über die zyklischen Körper vom Grad p^n (Albert, Witt), er geht dann durch das nichtkommutative Gebiet der zyklischen Algebren vom Grad p und p^n (H. L. Schmid), und endet schließlich wieder kommutativ mit Charakteristik 0, nämlich bei den Henselschen p-adischen Körpern (Hasse, F. K. Schmidt, Teichmüller, Witt) [1]).

Artin untersuchte die Körper der Charakteristik 0, die durch Adjunktion einer einzigen Zahl algebraisch abgeschlossen werden, und fand u. a., daß dies durch Adjunktion von $\sqrt{-1}$ geschehen kann. Um nun zu beweisen, daß ein algebraisch abgeschlossener Körper der Charakteristik p in bezug auf keinen Unterkörper von endlichem Grad ist, mußte gezeigt werden, daß bei Charakteristik p ein zyklischer Körper p-ten Grades immer enthalten ist in einem zyklischen Körper vom Grad p^2. Nebenresultate waren dabei die Artin-Schreiersche Normalform $x^p - x = a$ für die zyklischen Körper vom Grad p^2. Durch die Fortsetzung der hierfür entwickelten Methoden konnte Albert die zyklischen Körper vom Grad p^n schrittweise aufbauen. Es gelang mir, eine von speziellen Formeln freie Konstruktion anzugeben.

Inzwischen hatte H. L. Schmid die zyklischen Algebren p-ten Grades der Charakteristik p untersucht. Für diese Algebren $(\alpha, \beta]$ mit den Erzeugenden u, θ und den definierenden Relationen

$$u^p = \alpha, \quad \theta^p - \theta = \beta, \quad u\theta u^{-1} = \theta + 1$$

gelten die Regeln

$$(\alpha, \beta] \cdot (\alpha', \beta] \sim (\alpha\alpha', \beta] \text{ und } (\alpha, \beta] \cdot (\alpha, \beta'] \sim (\alpha, \beta + \beta'].$$

Für den Fall, daß der Grundkörper k aus Potenzreihen der Variablen t bestand, bewies Schmid die Residuenformel

$$(\alpha, \beta] \sim \left(t, \operatorname{Res} \frac{d\alpha}{\alpha} \beta\right].$$

Um entsprechende Resultate für Algebren vom Grad p^n zu erhalten, mußte zuerst meine sehr willkürliche Konstruktion für zyklische Körper vom Grad p^n wieder zweck-

[1]) Literaturangaben befinden sich auf S. 127.

mäßig normiert werden. Für p^2 fand Teichmüller eine Normierung. Eine andere wurde von Schmid gefunden und nach mühsamer Untersuchung auch für p^n. Für die entsprechend gebildeten zyklischen Algebren $(\alpha|\beta_0, \ldots, \beta_{n-1}]$ fand Schmid Regeln von der Form

$$(\alpha|\beta_i] \cdot (\alpha'|\beta_i] \sim (\alpha\alpha'|\beta_i] \quad \text{und} \quad (\alpha|\beta_i] \cdot (\alpha|\beta_i'] \sim (\alpha|s_i(\beta_j, \beta_j')]$$

mit gewissen Polynomen $s_i(x_j, y_j)$. Diese Polynome wurden zunächst für Charakteristik 0 definiert, und erst nach einem Beweis ihrer Ganzzahligkeit mod p genommen. Leider waren die Schmidschen Beweise durch Verwendung von Funktionen von vielen komplizierten Argumenten recht unübersichtlich.

Im Anschluß an die Schmidschen Untersuchungen machte ich die Entdeckung, daß die Verknüpfung $(x_i) + (y_i) = (s_i)$ mit Hilfe der Polynome $s_i(x_j, y_i)$ eine kommutative Gruppe der Vektoren $(x_i) = (x_0, x_1, \ldots)$ lieferte, die eng zusammenhing mit der Addition der p-adischen Zahlen $\Sigma\, x_i p^i$. Ausgehend von dieser Gruppe ließen sich jetzt die Schmidschen Resultate in vereinfachter Form herleiten. Ferner fand sich ein Analogon zur Residuenformel für den Grad p^n, wonach ich schon über ein Jahr lang gesucht hatte.

Die Gruppe der Vektoren mit Komponenten $\mathfrak{x}_i$ aus dem Körper von p Elementen erwies sich wirklich als identisch mit der Additionsgruppe der ganzen p-adischen Zahlen $\Sigma\, x_i p^i$ mit passendem Vertreter x_i der Restklasse $\mathfrak{x}_i$ mod p, und zwar waren nach einer Bemerkung von Hasse Vertreter x_i mit $x_i^p = x_i$ zu nehmen.

Da Teichmüller inzwischen auch eine neue Multiplikation der Vektoren fand, konnte er damit p-adische Körper mit beliebigem vollkommenen Restklassenkörper der Charakteristik p herstellen. Umgekehrt bewies Teichmüller den Satz, daß es in jedem diskret bewerteten perfekten Körper mit vollkommenem Restklassenkörper der Charakteristik p ein einziges Repräsentantensystem R mit der Eigenschaft $R^p = R$ gibt. Gestützt auf diesen Satz konnte er nun die Sätze von Hasse und F. K. Schmidt über die Struktur der diskret bewerteten perfekten Körper in neuer und viel einfacherer Form beweisen. Den verzweigten Fall konnte anschließend Hasse erledigen.

Auch diese Untersuchungen sind in dieser Arbeit aufgenommen worden, da sich unterdessen herausgestellt hat, daß alle Vektoroperationen gleichzeitig eingeführt werden können, und zwar in einer Weise, die jeden Nachweis von Rechengesetzen überflüssig macht. Außerdem werden dadurch die Beweise über die Struktur der diskret bewerteten perfekten Körper noch weiter vereinfacht.

Überraschend ist der enge Zusammenhang der Theorie der zyklischen Körper und Algebren der Charakteristik p vom Grad p^n mit der p-adischen Addition. Und noch mehr überrascht *die Erkenntnis, daß die Addition und Multiplikation der p-adischen Zahlen sich in einem Körper der Charakteristik p rational begründen läßt.*

Literaturverzeichnis.

1. A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Am. Math. Soc. **40** (1934).
2. E. Artin, Kennzeichnung des Körpers der reellen algebraischen Zahlen, Abh. Math. Sem. Hamburg **3** (1924).
3. E. Artin und O. Schreier, Über eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Hamburg **5** (1927).
4. H. Hasse und F. K. Schmidt, Die Struktur diskret bewerteter Körper, Crelle **170** (1934).
5. H. L. Schmid, Zyklische algebraische Funktionenkörper vom Grad p^n über endlichem Konstantenkörper der Charakteristik p, Crelle **175** (1936).
6. O. Teichmüller, Über die Struktur diskret bewerteter perfekter Körper, Gött. Nachr. 1936.
7. E. Witt, Der Existenzsatz für abelsche Funktionenkörper, Crelle **173** (1935). — Die Resultate dieser Arbeit werden mit W. I, 2; W. II; W. III usw. zitiert.
8. E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^l, Crelle **174** (1936).

1. Begründung einer Vektorrechnung.

p sei eine feste Primzahl. Für einen *Vektor*

$$x = (x_0, x_1, x_2, \ldots)$$

mit abzählbar vielen *Komponenten* x_n führen wir *Nebenkomponenten*

(a) $$x^{(n)} = x_0^{p^n} + p x_1^{p^{n-1}} + \cdots + p^n x_n$$

ein und bringen das auch gelegentlich in der Schreibweise

$$x = (x_0, x_1, x_2, \ldots \mid x^{(0)}, x^{(1)}, x^{(2)}, \ldots)$$

zum Ausdruck. Da sich umgekehrt x_n rekursiv als rationalzahliges Polynom in $x^{(0)}, \ldots, x^{(n)}$ aus den Gleichungen (a) berechnen läßt, ist ein Vektor x auch schon durch Angabe seiner Nebenkomponenten völlig bestimmt.

Summe, Differenz und Produkt zweier Vektoren erklären wir *nebenkomponentenweise*:

(b) $$x \dot{\pm} y = (?, ?, \ldots \mid x^{(0)} \dot{\pm} y^{(0)}, x^{(1)} \dot{\pm} y^{(1)}, \ldots).$$

Wir wollen nun einige besondere Regeln für das Rechnen mit Vektoren herleiten. Dazu führen wir das *Verschiebungszeichen* V ein durch

(1) $$Vx = (0, x_0, x_1, \ldots).$$

Zur Abkürzung setzen wir noch

(2) $$\{u\} = (u, 0, 0, \ldots),$$

es ist also $V^i\{u\}$ ein Vektor, dessen i-te Komponente gleich u und dessen übrige Komponenten 0 sind. Aus (a) folgt

(c) $$(Vx)^{(n)} = p x^{(n-1)} \qquad (x^{(-1)} = 0)$$

oder ausführlich geschrieben

(d) $$Vx = (0, x_0, x_1, \ldots \mid 0, p x^{(0)}, p x^{(1)}, \ldots).$$

Es bestehen die Regeln

(3) $$V(x + y) = Vx + Vy$$

(4) $$(x_0, x_1, x_2, \ldots) = \sum_0^{r-1} V^i\{x\} + V^r(x_r, x_{r+1}, \ldots),$$

(5) $$\{u\}\,(x_0, x_1, x_2, \ldots) = (u x_0, u^p x_1, u^{p^2} x_2, \ldots),$$

wie man sofort durch Hinschreiben der n-ten Nebenkomponenten bestätigt. Es liegt nahe, die folgenden Bezeichnungen einzuführen:

(6) $$\begin{aligned} \mathbf{0} &= (0, 0, 0, \ldots) \\ \mathbf{1} &= (1, 0, 0, \ldots) \\ \boldsymbol{m} &= \mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}. \end{aligned}$$

Weiter wollen wir die fraglichen Komponenten $(x \dot{\pm} y)_n$ des Vektors $x \dot{\pm} y$ näher untersuchen. Dazu setzen wir

(7) $$x^p = (x_0^p, x_1^p, x_2^p, \ldots).$$

x^p ist also nicht etwa die p-te Potenz im Sinn der Vektormultiplikation; diese wird gar nicht vorkommen. Aus (a) folgt die *Rekursionsgleichung*

(e) $$x^{(n)} = x^{p(n-1)} + p^n x_n,$$

wobei natürlich $x^{p(n-1)}$ die $(n-1)$-te Nebenkomponente des Vektors x^p bedeutet und nicht etwa eine $p(n-1)$-te Potenz.

Wir bezeichnen allgemein mit

$$R[u, v, \ldots] \text{ und } G[u, v, \ldots]$$

den Ring aller rationalzahligen bzw. ganzzahligen Polynome in $u, v, \ldots$.

Aus (e) und (b) folgt die additive Kongruenz

$$p^n(x+y)^n \equiv (x+y)^{(n)} = x^{(n)} + y^{(n)} \equiv p^n x_n + p^n y_n \bmod R[x_0, y_0, \ldots, x_{n-1}, y_{n-1}],$$

also mit einem passenden Polynom f

$$(8) \qquad (x+y)_n = x_n + y_n + f(x_0, y_0, \ldots, x_{n-1}, y_{n-1}).$$

Bisher haben wir die Vektoroperationen nur *algebraisch* untersucht, und an keiner Stelle wurde benutzt, daß p eine Primzahl ist. Wir kommen jetzt auf die *arithmetischen* Eigenschaften zu sprechen, die aus der besonderen Gestalt der Gleichungen (a) fließen. Wir zeigen dazu das

Lemma. *Für zwei Vektoren x und y mögen die Hauptkomponenten in einem Integritätsbereich $\mathfrak{J}$ der Charakteristik 0 liegen. Dann sind für $r > 0$ die Kongruenzen*

$$x_\nu \equiv y_\nu \bmod p^r \mathfrak{J}$$

gleichwertig mit den Kongruenzen

$$x^{(\nu)} \equiv y^{(\nu)} \bmod p^{r+\nu} \mathfrak{J}.$$

Beweis. Für $\nu < n$ sei die Gleichwertigkeit schon erkannt, also dürfen wir annehmen, es sei $x_\nu \equiv y_\nu \bmod p^r \mathfrak{J}$. Wegen $x_\nu^p \equiv y_\nu^p \bmod p^{r+1} \mathfrak{J}$ folgt nach Induktionsnahme

$$x^{p(n-1)} \equiv y^{p(n-1)} \bmod p^{r+n} \mathfrak{J}.$$

Nun ist wegen (e)

$$(x^n - y^n) - (p^n x_n - p^n y_n) = x^{p(n-1)} - y^{p(n-1)} \equiv 0 \bmod p^{r+n} \mathfrak{J},$$

und daraus folgt die Gleichwertigkeit auch für $\nu = n$.

Satz 1. $(x \dot{\pm} y)_n$ *ist ein ganzzahliges Polynom in* $x_0, y_0, \ldots, x_n, y_n$.

In den beiden ersten Komponenten ist beispielsweise

$$x + y = \left(x_0 + y_0,\ x_1 + y_1 - \sum_1^{p-1} \frac{1}{p} \binom{p}{\nu} x_0^\nu y_0^{p-\nu},\ \text{usw.}\right)$$

$$x \cdot y = (x_0 y_0,\ x_1 y_0^p + x_0^p y_1 + p x_1 y_1,\ \text{usw.})$$

Beweis. $x^{(n)}$ und $y^{(n)}$ liegen im Ring $\mathfrak{J} = G[x_0, y_0 \ldots, x_n, y_n]$. Nach (e) ist

$$x^{(n)} \equiv x^{p(n-1)} \text{ und } y^{(n)} \equiv y^{p(n-1)} \bmod p^n \mathfrak{J}.$$

Daher ist wegen (b)

$$(x \dot{\pm} y)^{(n)} = x^{(n)} \dot{\pm} y^{(n)} \equiv x^{p(n-1)} \dot{\pm} y^{p(n-1)} = (x^p \dot{\pm} y^p)^{(n-1)} \bmod p^n \mathfrak{J}.$$

Für $\nu < n$ sei der Satz schon bewiesen, also gilt $(x \dot{\pm} y)_\nu^p \equiv (x^p \dot{\pm} y^p)_\nu \bmod p\,\mathfrak{J}$. Das Lemma ergibt

$$(x \dot{\pm} y)^{p(n-1)} \equiv (x^p \dot{\pm} y^p)^{(n-1)} \bmod p^n \mathfrak{J}.$$

Wegen (e) ist

$$p^n (x \dot{\pm} y)_n = (x \dot{\pm} y)^{(n)} - (x \dot{\pm} y)^{p(n-1)} \equiv 0 \bmod p^n \mathfrak{J},$$

und daraus folgt der Satz auch für $\nu = n$.

Satz 2. *Es gilt komponentenweise* $\boldsymbol{p}x \equiv Vx^p \bmod pG[x_i]$.

Beweis. Nach (e), (c), (b), ist für die Nebenkomponenten

$$(\boldsymbol{p}x)^{(n)} = px^{(n)} \equiv px^{p(n-1)} = (Vx^p)^{(n)} \bmod p^{n+1} G[x_i],$$

aus dem Lemma folgt jetzt die Behauptung $(\boldsymbol{p}x)_n \equiv (Vx^p)_n \bmod pG[x_i]$.

2. Der Residuenvektor (α, β).

Zur Vorbereitung für die letzten Abschnitte müssen wir die folgenden Betrachtungen einschalten.

Wir betrachten formale Potenzreihen

$$\alpha = a_m t^m + a_{m+1} t^{m+1} + \cdots \qquad (a_m \neq 0)$$

in t mit Koeffizienten a_i aus einem Integritätsbereich $\mathfrak{J}$ der Charakteristik 0. β sei ein Vektor, dessen einzelne Komponenten β_ν wieder Potenzreihen [2]) sind:

$$\beta = (\beta_0, \beta_1, \ldots), \qquad \beta_\nu = \sum_{i>-\infty} b_{\nu i} t^i.$$

Für den von α und β abhängigen Vektor

$$(f) \qquad (\alpha, \beta) = \left(?, ?, \ldots \,\middle|\, \operatorname{Res} \frac{d\alpha}{\alpha} \beta^{(0)}, \operatorname{Res} \frac{d\alpha}{\alpha} \beta^{(1)}, \ldots\right)$$

gelten nach (e) und (d) die Rechenregeln

$$(9) \qquad (\alpha\alpha', \beta) = (\alpha, \beta) + (\alpha', \beta),$$

$$(10) \qquad (\alpha, \beta + \beta') = (\alpha, \beta) + (\alpha, \beta'),$$

$$(11) \qquad (\alpha, V\beta) = V(\alpha, \beta).$$

Für später sprechen wir die unmittelbar aus (f) folgenden Tatsachen aus:

Satz 3. *Ist c ein Vektor mit lauter konstanten Komponenten, so gilt $(\alpha, \beta) \cdot c = (\alpha, \beta c)$. Es ist $(t, c) = c$. Enthalten alle Entwicklungen der β_ν nur Potenzen von t mit lauter positiven bzw. lauter negativen Exponenten, so ist $(t, \beta) = 0$.*

Wir zeigen nun den folgenden arithmetischen

Satz 4. *Für*

$$\alpha = a_m t^m + a_{m+1} t^{m+1} + \cdots \qquad (a_m \neq 0),$$

$$\beta = (\beta_0, \beta_1, \ldots) \quad \textit{mit} \quad \beta_\nu = \sum_{i>-\infty} b_{\nu i} t^i$$

sind die Komponenten $(\alpha, \beta)_n$ des Vektors (α, β) ganzzahlige Polynome in a_m^{-1}, a_i, $b_{\nu i}$.

Beweis. Es sei $\mathfrak{J} = G[a_m^{-1}, a_i, b_{\nu i}]$.

Wir führen zunächst den Beweis durch für den Fall $\alpha = t$. Zum Vektor β bilden wir die Vektoren β' und β'' mit den Komponenten

$$\beta'_\nu = \sum_{i>0} b_{\nu i} t^i \quad \text{bzw.} \quad \beta''_\nu = \sum_{i<0} b_{\nu i} t^i,$$

und führen damit die Vektoroperation Ω ein durch

$$\Omega\beta = \beta - \beta' - \beta''.$$

Mit den Koeffizienten von β liegen nach Satz 1 auch die Koeffizienten von $\Omega\beta$ in $\mathfrak{J}$. Sind die Komponenten $\beta_0, \ldots, \beta_{\nu-1}$ konstant, so auch die Komponenten $(\Omega\beta)_0, \ldots, (\Omega\beta)_\nu$. Nach (10) und Satz 3 ist

$$(t, \Omega\beta) = (t, \beta) - (t, \beta') - (t, \beta'') = (t, \beta),$$

und deshalb allgemein $(t, \beta) = (t, \Omega^n\beta)$. Für $\nu < n$ ist nun $(\Omega^n\beta)_\nu$ konstant; wie in Satz 3 gilt daher $(t, \Omega^n\beta)_\nu = (\Omega^n\beta)_\nu$. Somit liegt

$$(t, \beta)_\nu = (\Omega^n\beta)_\nu \qquad (\nu < n)$$

im Integritätsbereich $\mathfrak{J}$.

Nun sei α eine beliebige Potenzreihe. Wir können β_ν nach der neuen Variablen

---

[2]) Die Summationsbezeichnung $\sum_{i>-\infty}$ soll andeuten, daß in der Reihe nur endlich viele Glieder mit negativem Index i auftreten.

$t' = t^{1-m}\alpha$ entwickeln, und zwar liegen die neuen Koeffizienten $b'_{\nu i}$ wieder in $\mathfrak{J}$. Nach dem vorhin Bewiesenen ist $(t', \beta)_n$ ganzzahliges Polynom in $b'_{\nu i}$, liegt also in $\mathfrak{J}$. Nach (9) und (10) gilt die Zerlegung

$$(\alpha, \beta) = (\boldsymbol{m} - \mathbf{1}) \cdot (t, \beta) + (t', \beta),$$

nach Satz 1 liegen daher die Komponenten des Vektors (α, β) ebenfalls in $\mathfrak{J}$, w. z. b. w.

3. Vektoren bei Charakteristik p. Konstruktion von p-adischen Körpern.

Theoretisch brauchen wir nur die ganzzahligen Polynome $(x \dot{\pm} y)_n$ einfach anzugeben und können dann mit ihnen Summe, Differenz und Produkt von Vektoren erklären, ohne überhaupt von Nebenkomponenten zu reden. In diesem Sinn muß das bestehende Distributivgesetz $x(y+z) = xy + xz$ als Zusammenfassung von ganzzahligen Polynomidentitäten in x_i, y_i, z_i angesehen werden. Ähnlich ist es mit den anderen Gesetzen. Ebenso würde es genügen, wenn wir die ganzzahligen Polynome $(\alpha, \beta)_n$ einfach angeben. Die Formeln (1) bis (11) und die Sätze 1 bis 4 behalten dann ihre Gültigkeit.

Diesen Standpunkt nehmen wir nun ein und betrachten alles mod p:

Erklärung. *$x \dot{\pm} y$ ist ein Vektor, dessen Komponenten feststehende Polynome in x_i, y_i sind mit Koeffizienten aus dem Galoisfeld $GF(p)$ von p Elementen. Es gelten die Kommutativ-, Assoziativ- und Distributivgesetze.*

(α, β) ist ein Vektor, dessen Komponenten feststehende Polynome in $a_m^{-1}, a_i, b_{\nu i}$ sind mit Koeffizienten aus $GF(p)$.

Die Formeln (1) *bis* (11) *und Satz* 3 *bleiben bestehen. Ferner gilt jetzt*

$$(x \dot{\pm} y)^p = x^p \dot{\pm} y^p, \tag{12}$$

$$\boldsymbol{p}x = Vx^p \qquad \text{(Satz 2)}, \tag{13}$$

$$(V^i x) \cdot (V^j y) = V^{i+j}(x^{p^j} y^{p^i}). \tag{14}$$

Um (14) zu beweisen, dürfen wir erst x und y durch x^{p^i}, y^{p^j} ersetzen. Dann geht die Behauptung wegen (13) über in $(\boldsymbol{p}^i x) \cdot (\boldsymbol{p}^j y) = \boldsymbol{p}^{i+j}(xy)$.

Nun sei $\mathfrak{k}$ ein **beliebiger Körper der Charakteristik p.** Wir betrachten Vektoren x mit Komponenten aus $\mathfrak{k}$. Diese bilden hinsichtlich der erklärten Vektorrechnung einen Ring $I(\mathfrak{k})$. Diesen Ring wollen wir nunmehr untersuchen.

Wir definieren folgendermaßen eine Bewertung der Vektoren:

Es werde $|x| = p^{-r}$ gesetzt, wenn x_r die erste von Null verschiedene Komponente des Vektors x ist; ferner $|0| = 0$. Aus (3) und (14) folgen dann sofort die beiden Regeln

$$|x + y| \leqq \mathrm{Max}\,(|x|, |y|), \tag{15}$$

$$|xy| = |x| \cdot |y|. \tag{16}$$

Auf Grund dieser Bewertung dürfen wir von Konvergenz reden. Nach (4) gilt jetzt

$$(x_0, x_1, x_2, \ldots) = \sum_0^\infty V^i\{x_i\}. \tag{17}$$

Es ist ohne weiteres klar, daß jede konvergente Folge von Vektoren gegen einen Vektor konvergiert, d. h. daß der Ring $I(\mathfrak{k})$ perfekt ist.

Satz 5. *Im Ring $I(\mathfrak{k})$ ist ein Vektor $a = (a_0, a_1, \ldots)$ mit $a_0 \neq 0$ eine Einheit.*

Beweis. Setzen wir nämlich $\mathbf{1} - a\{a_0^{-1}\} = Vb$, so ist

$$a \cdot \{a_0^{-1}\} \sum_0^\infty (Vb)^i = (\mathbf{1} - Vb) \sum_0^\infty (Vb)^i = \mathbf{1}.$$

Jetzt sei $\mathfrak{k}$ ein **vollkommener Körper der Charakteristik p.** Wir haben dann für jeden Vektor aus dem Ring $I(\mathfrak{k})$ die Reihenentwicklung

$$(x_0, x_1, x_2, \ldots) = \sum_0^\infty p^i \{x^{p^{-i}}\}.$$

Wir wollen nun den Quotientenkörper $Q(\mathfrak{k})$ des Rings $I(\mathfrak{k})$ bilden. Da die in $Q(\mathfrak{k})$ gebildeten Reihen

$$\sum_{i>-\infty} p^i \{x^{p^{-i}}\} \tag{18}$$

offensichtlich einen Körper bilden, besteht $Q(\mathfrak{k})$ gerade aus allen Reihen (18). Wie immer, so läßt sich auch hier die Bewertung auf den Quotientenkörper fortsetzen.

Satz 6. *Für einen vollkommenen Körper $\mathfrak{k}$ ist der Quotientenkörper $Q(\mathfrak{k})$ des Ringes $I(\mathfrak{k})$ aller Vektoren aus $\mathfrak{k}$ ein diskret bewerteter perfekter Körper der Charakteristik* 0. *$Q(\mathfrak{k})$ ist unverzweigt, d. h. (p) ist ein Primideal in $I(\mathfrak{k})$. Der Restklassenkörper $I(\mathfrak{k})/(p)$ ist mit $\mathfrak{k}$ isomorph.*

Diskrete Bewertung bedeutet dabei: die vorkommenden Beträge haben *nur* den Häufungspunkt 0.

4. Struktur diskret bewerteter perfekter Körper.

Diesen Abschnitt schalten wir ein, um eine Übersicht über alle diskret bewerteten perfekten Körper $\mathfrak{k}$ mit vollkommenem Restklassenkörper $\mathfrak{k}$ der Charakteristik p zu gewinnen.

Es sei k ein bewerteter perfekter Körper. Für den Betrag mögen die Regeln (15) und (16) gelten. Die vorkommenden Beträge sollen nur den Häufungspunkt 0 haben. Die Elemente a mit $|a| \leqq 1$ (ganze Elemente) bilden einen Integritätsbereich $\mathfrak{J}$. Die Elemente b mit $|b| < 1$ bilden in $\mathfrak{J}$ ein Primideal, wegen der Diskretheit der Bewertung ist es ein Hauptideal (π). Der Restklassenkörper $\mathfrak{k} = \mathfrak{J}/(\pi)$ sei ein vollkommener Körper der Charakteristik p. Da für eine Primzahl $q \neq p$ sicher $q \not\equiv 0 \bmod \pi$, also erst recht $q \not\equiv 0$ in k ist, hat k entweder die Charakteristik p oder die Charakteristik 0.

Für die Beweise der nachfolgenden Sätze 7 und 9 machen wir zwei Feststellungen:

(g) Für ganze Elemente a und b folgt aus $a \equiv b \bmod \pi^r$ $(r > 0)$ die Kongruenz $a^{p^n} \equiv b^{p^n} \bmod \pi^{r+n}$ $(n \geqq 0)$.

(h) Sind die Komponenten der Vektoren x und y ganz, so folgt aus den Kongruenzen $x_\nu \equiv y_\nu \bmod \pi^r$ $(r > 0)$ die Kongruenz $x^{(n)} \equiv y^{(n)} \bmod \pi^{r+n}$ $(n \geqq 0)$.

Weil nämlich $\binom{p}{i} \equiv 1$ oder $0 \bmod \pi$ ist, folgt zunächst $a^p \equiv b^p \bmod \pi^{r+1}$ und dann durch n-malige Iteration die Behauptung (g). Hiermit läßt sich aus der Gleichung (a) unmittelbar die andere Behauptung (h) ablesen. —

Mit einem Repräsentantensystem R aus $\mathfrak{J} \bmod \pi$ läßt sich jedes Element aus k auf genau eine Weise in eine Reihe

$$\sum_{i>-\infty} r_i \pi^i \qquad (r_i \text{ aus } R) \tag{19}$$

entwickeln.

Wir zeigen nun nach Teichmüller:

Satz 7. *Es gibt in $\mathfrak{J}$ ein einziges Repräsentantensystem R mit der Eigenschaft $R^p = R$. Es ist multiplikativ abgeschlossen. Wenn k die Charakteristik p hat, so ist R ein mit $\mathfrak{k}$ isomorpher Körper.*

Beweis. $\mathfrak{a}$ sei eine feste Restklasse $\bmod \pi$. Wir wählen aus jeder Restklasse $\mathfrak{a}^{p^{-\nu}}$ $(\nu \geqq 0)$ ein beliebiges Element a_ν, und behaupten: $a_\nu^{p^\nu}$ konvergiert für $\nu \to \infty$, und zwar gegen eine Zahl a aus $\mathfrak{a}$, und weiter, a hängt nicht ab von der besonderen Auswahl der a_ν.

Es folgt nämlich $a_{\nu+1}^{p} \equiv a_\nu \bmod \pi$, also $a_{\nu+1}^{p^{\nu+1}} \equiv a_\nu^{p^\nu} \bmod \pi^{\nu+1}$, und hieraus folgt die Konvergenz. Weil jedes $a_\nu^{p^\nu}$ in $\mathfrak{a}$ liegt, muß auch der Grenzwert a darin liegen. a_ν' seien die Elemente einer zweiten Auswahl. Wegen $a_\nu' \equiv a_\nu \bmod \pi$ ist $a_\nu'^{p^\nu} \equiv a_\nu^{p^\nu} \bmod \pi^{\nu+1}$, und für die Grenzwerte folgt $a' = a$.

Konstruieren wir für jede Restklasse $\mathfrak{a}$ die zugehörige Zahl a, so bilden diese Zahlen ein Repräsentantensystem R. Es sei $\mathfrak{a}\,\mathfrak{b} = \mathfrak{c}$. Dann liegt $a_\nu b_\nu = c_\nu$ in $\mathfrak{a}^{p^{-\nu}}\,\mathfrak{b}^{p^{-\nu}} = \mathfrak{c}^{p^{-\nu}}$, und wegen $a^{p^\nu} b^{p^\nu} = c^{p^\nu}$ folgt für die Grenzwerte $a\,b = c$. Daher ist R multiplikativ abgeschlossen, und wegen $\mathfrak{k}^p = \mathfrak{k}$ ist $R^p = R$. Wenn k die Charakteristik p hat, so folgt analog aus $\mathfrak{a} + \mathfrak{b} = \mathfrak{c}$ die Gleichung $a + b = c$, also ist R ein mit $\mathfrak{k}$ isomorpher Körper.

Umgekehrt sei R' ein Repräsentantensystem mit $R'^p = R$. Es sei a_ν' der Repräsentant aus $\mathfrak{a}^{p^{-\nu}}$, dann ist $a_\nu'^{p^\nu} = a_0'$, also der Grenzwert $a = a_0'$, d. h. es ist $R = R'$.

Aus diesem Satz in Verbindung mit (19) folgt

Satz 8. *Ein diskret bewerteter perfekter Körper k der Charakteristik p mit einem vollkommenen Restklassenkörper $\mathfrak{k}$ der Charakteristik p ist mit einem Potenzreihenkörper einer Variablen über $\mathfrak{k}$ isomorph.*

Nunmehr habe k die Charakteristik 0. Es sei $(p) = (\pi^e)$, wegen $p \equiv 0 \bmod \pi$ ist $e > 0$.

Satz 9. *Jedem Vektor*

$$\mathfrak{x} = (\mathfrak{x}_0, \mathfrak{x}_1, \ldots)$$

aus $I(\mathfrak{k})$ werde die ganze Zahl

$$\xi = \sum_0^\infty x_i^{p^{-i}}\, p^i$$

aus k zugeordnet, wobei $x_i^{p^{-i}}$ der Repräsentant von $\mathfrak{x}_i^{p^{-i}}$ in dem Repräsentantensystem R mit $R^p = R$ ist.

Aus $\mathfrak{x} \pm \mathfrak{y} = \mathfrak{z}$ folgt dann $\xi \pm \eta = \zeta$.

Beweis. Es werde $\mathfrak{x}^{p^{-n}} = (\mathfrak{x}_0^{p^{-n}}, \mathfrak{x}_1^{p^{-n}}, \ldots)$ und $x^{p^{-n}} = (x_0^{p^{-n}}, x_1^{p^{-n}}, \ldots)$ gebildet, wobei $x_i^{p^{-n}}$ wieder in R liegen und $\mathfrak{x}_i^{p^{-n}}$ repräsentieren soll. — Nach (a) ist

$$x^{p^{-n}(n)} = \sum_0^n x^{p^{-i}}\, p^i,$$

also

$$\lim x^{p^{-n}(n)} = \xi.$$

Aus $\mathfrak{x} \pm \mathfrak{y} = \mathfrak{z}$ folgt $\mathfrak{x}^{p^{-n}} \pm \mathfrak{y}^{p^{-n}} = \mathfrak{z}^{p^{-n}}$, und hieraus $(x^{p^{-n}} \pm y^{p^{-n}})_\nu \equiv z_\nu^{p^{-n}} \bmod \pi$. Nach (b) und (h) ergibt sich für die Nebenkomponenten

$$x^{p^{-n}(n)} \pm y^{p^{-n}(n)} = (x^{p^{-n}} \pm y^{p^{-n}})^{(n)} \equiv z^{p^{-n}(n)} \bmod \pi^{n+1}.$$

Für die Grenzwerte ist daher $\xi \pm \eta = \zeta$, w. z. b. w.

Damit ist gezeigt, daß die Reihen $\sum_0^\infty R p^i$ $(R^p = R)$ einen zu $I(\mathfrak{k})$ isomorphen Ring $\mathfrak{J}'$ bilden. Folglich bilden die Reihen $\sum_{i > -\infty} R p^i$ einen zu $Q(\mathfrak{k})$ isomorphen Körper k'.

Wie jedes Element aus $\mathfrak{J}$ läßt sich auch π^e/p in eine Reihe

$$\frac{\pi^e}{p} = \sum_{i=0}^{r-1} \sum_{j=0}^{\infty} r_{ij}\, p^j \pi^i = \sum_{i=0}^{r-1} g_i \pi^i$$

entwickeln mit r_{ij} aus $R^p = R$, bzw. g_i aus $\mathfrak{J}'$. Mit π^e/p muß auch g_0 prim zu p sein. Es ist also $k = k'(\pi)$, wobei π einer Eisensteinschen Gleichung e-ten Grades genügt.

Satz 10. *Ein diskret bewerteter perfekter Körper der Charakteristik* 0 *mit einem vollkommenen Restklassenkörper* $\mathfrak{k}$ *der Charakteristik* p *enthält einen invariant bestimmten Unterkörper* k', *der zum Körper* $Q(\mathfrak{k})$ *von Satz* 6 *isomorph ist. Ist* $(p) = (\pi^e)$ *mit einem Primelement* π *aus* k, *so ist* $k = k'(\pi)$, *wo* π *einer Eisensteinschen Gleichung* e*-ten Grades genügt.*

Während die Sätze 8 und 10 die Struktur der diskret bewerteten perfekten Körper mit vollkommenem Restklassenkörper $\mathfrak{k}$ aufdecken, kann uns Satz 9 dazu dienen, gegebenenfalls das Rechnen mit Vektoren zurückzuführen auf das Rechnen mit ganzen p-adischen Zahlen.

5. Zyklische und abelsche Körper der Charakteristik p vom Exponenten p^n.

Es sei k ein beliebiger Körper der Charakteristik p. Wir wollen seine zyklischen Oberkörper vom Grad p^n, allgemeiner seine abelschen Oberkörper vom Exponenten p^n untersuchen.

Dazu rechnen wir mit Vektoren x mit Komponenten aus k, und zwar nur mod V^n, d. h. wir rechnen nur mit Vektoren

$$x = (x_0, x_1, \ldots, x_{n-1})$$

der Länge n.

Wir gehen jetzt genau nach derselben Methode vor wie in der Arbeit W. I, nur daß wir alle dort bewiesenen Sätze über Körperzahlen hier entsprechend für Vektoren aussprechen.

Mit $\sigma, \tau, \ldots$ seien die Automorphismen des galoisschen (separablen) Körpers K/k bezeichnet. Für einen Vektor $C = (C_0, C_1, \ldots)$ mit C_i aus K erklären wir

$$C^\sigma = \sigma C = (\sigma C_0, \sigma C_1, \ldots)$$
$$\mathrm{Sp}\, C = \sum_\sigma \sigma C = (\mathrm{Sp}\, C_0, \ *\ , \ldots).$$

Ist also C_0 eine Zahl, deren Spur nicht verschwindet, so gibt es nach Satz 5 einen zu Sp C reziproken Vektor. Es bestehen die Regeln

$$\sigma(A + B) = \sigma A + \sigma B, \qquad (AB)^\sigma = A^\sigma B^\sigma.$$

Jedem σ sei ein Vektor A_σ zugeordnet. Der Satz W. I, 2 kann mitsamt seinem Beweis fast ungeändert übernommen werden:

Satz 11. *Bestehen die Relationen* $A_\sigma + \sigma A_\tau = A_{\sigma\tau}$, *so gibt es einen solchen Vektor* B, *daß* $A_\sigma = (1 - \sigma)\ B$ *gilt.*

Zum Beweis nehmen wir den oben konstruierten Vektor C. Wie man leicht nachrechnet, kann $B = \dfrac{1}{\mathrm{Sp}\, C} \sum_\tau A_\tau\, \tau C$ gewählt werden.

Übrigens gelten auch hier die Sätze W. I, 1 und W. I, 3.

Ebenso wie für Zahlen a vorteilhaft die Bezeichnung $\wp a = a^p - a$ eingeführt wurde, setzen wir für Vektoren

$$\wp x = x^p - x = (x_0^p, x_1^p, \ldots, x_{n-1}^p) - (x_0, x_1, \ldots, x_{n-1}).$$

Es besteht die Regel

$$\wp(x + y) = \wp x + \wp y.$$

Die Lösungen von $\wp x = 0$ sind genau die Vektoren mit Komponenten aus dem Primkörper.

Wir nennen nun die Vektoren α von der Form $\wp\beta$ zerfallend, und schreiben dafür auch $\alpha \sim 0$.

1. Der Zerfall von $(0, \alpha_1, \ldots, \alpha_{n-1})$ ist gleichwertig mit dem Zerfall von $(\alpha_1, \ldots, \alpha_{n-1})$.

Denn ist $(0, \alpha_1, \ldots, \alpha_{n-1}) = \wp(\beta_0, \beta_1, \ldots, \beta_{n-1})$, so liegt β_0 im Primkörper. Wird die Gleichung $0 = \wp(\beta_0, 0 \ldots, 0)$ abgezogen, so bleibt

$$(0, \alpha_1, \ldots, \alpha_{n-1}) = \wp(0, \beta_1, \ldots, \beta_{n-1}),$$

und diese Gleichung ist nach (4) gleichwertig mit $(\alpha_1, \ldots, \alpha_{n-1}) = \wp(\beta_1, \ldots, \beta_{n-1})$.

2. Im algebraisch abgeschlossenen Körper $\bar{k}$ zerfällt jeder Vektor.

Denn in $\bar{k}$ darf man $\alpha_0 = \wp a$ setzen, und wegen

$$(20) \qquad (\wp a, \alpha_1, \ldots, \alpha_{n-1}) \sim (\wp a, \alpha_1, \ldots, \alpha_{n-1}) - \wp(a, 0, \ldots, 0) = (0, \alpha_1', \ldots, \alpha_{n-1}')$$

braucht jetzt nur noch der Zerfall des kürzeren Vektors $(\alpha_1', \ldots, \alpha_{n-1}')$ nachgewiesen zu werden.

Im Körper k können wir jedenfalls sagen, daß die Komponenten θ_i einer Lösung $\theta = (\theta_0, \ldots, \theta_{n-1})$ der Gleichung $\wp\theta = \alpha$ algebraische Zahlen sind. $K = K(\theta_0, \ldots, \theta_{n-1})$ ist also ein Zerfällungskörper des Vektors α. Jede weitere Lösung unterscheidet sich von θ nur um einen Vektor aus dem Primkörper, daher liegen in K sämtliche Lösungen. K ist also charakterisiert als kleinster Zerfällungskörper des Vektors α und muß daher galoissch sein. Die sämtlichen Lösungen θ der Gleichung $\wp\theta = \alpha$ sollen mit $\frac{1}{\wp}\alpha$ bezeichnet werden.

Wir sind nun im Stande, sämtliche Überlegungen und Sätze aus W. III (und W. II) fast wörtlich zu übertragen. Es ist dabei zu beachten, daß an Stelle von Zahlen immer Vektoren der Länge n zu nehmen sind, und statt einer Anwendung von W. I muß hier der vorhin bewiesene Satz 11 herangezogen werden. Auf diese Weise gelangen wir zu den Ergebnissen:

Satz 12. *Es sei ω eine additive Gruppe von Vektoren der Länge n, die alle zerfallenden Vektoren $\wp\alpha$ enthält, so daß $\omega/\wp\alpha$ endlich ist. Dann ist die galoissche Gruppe von $k\left(\frac{1}{\wp}\omega\right)/k$ zur Gruppe $\omega/\wp\alpha$ isomorph.*

Zu jedem abelschen Körper K/k vom Exponenten p^n gibt es genau eine solche Gruppe $\omega/\wp\alpha$, daß $K = k\left(\frac{1}{\wp}\omega\right)$ gilt.

Wir wollen nun zusehen, wie sich insbesondere die zyklischen Körper Z vom Grade p^n darstellen. Es ist $Z = k\left(\frac{1}{\wp}\beta\right)$ mit einem einzigen Vektor β der Länge n, und dabei darf $p^{n-1}\beta$ nicht zerfallen. Nun ist

$$(21) \qquad p\beta = V\beta^p = V\beta + \wp V\beta \sim V\beta,$$

also darf $V^{n-1}\beta$, d. h. β_0 nicht zerfallen. Ist θ eine Lösung von $\wp\theta = \beta$, so erhalten wir durch Anwendung der Automorphismen von Z/k auf θ genau p^n verschiedene, d. h. alle Lösungen dieser Gleichung. Daher gibt es einen Automorphismus σ mit $\sigma\theta = \theta + 1$. Wegen $\sigma^{p^{n-1}}\theta = \theta + p^{n-1} \neq \theta$ hat σ die Ordnung p^n.

Satz 13. *Ist $\beta = (\beta_0, \ldots, \beta_{n-1})$ ein Vektor mit $\beta_0 \neq \wp a$, so entsteht aus k durch Adjunktion einer Lösung $\theta = (\theta_0, \ldots, \theta_{n-1})$ der Gleichung $\wp\theta = \beta$ ein zyklischer Körper $Z = k\left(\frac{1}{\wp}\beta\right)$ vom Grad p^n.*

Umgekehrt läßt sich jeder zyklische Körper vom Grad p^n in dieser Weise darstellen. Durch $\sigma\theta = \theta + 1$ wird ein erzeugender Automorphismus von Z definiert.

6. Zyklische Algebren der Charakteristik p vom Grad p^n.

Wir werden jetzt die zyklischen Algebren vom Grad p^n über einem beliebigen Körper k der Charakteristik p behandeln.

Es sei $\alpha \neq 0$ eine Zahl und $\beta = (\beta_0, \ldots, \beta_{n-1})$ ein Vektor der Länge n aus k. Mit

$$(\alpha, \beta] = (\alpha \mid \beta_0, \ldots, \beta_{n-1}]$$

bezeichnen wir den **hyperkomplexen Ring**

mit der Erzeugenden u, den untereinander vertauschbaren Erzeugenden $\theta_0, \ldots, \theta_{n-1}$ und den definierenden Relationen $u^{p^n} = \alpha$, $\wp\theta = \beta$, $u\theta u^{-1} = \theta + \mathbf{1}$.

Dabei ist $\theta = (\theta_0, \ldots, \theta_{n-1})$ und $u\theta u^{-1} = (u\theta_0 u^{-1}, \ldots, u\theta_{n-1}u^{-1})$ gesetzt.

Die Transformation mit u liefert also einen Automorphismus des kommutativen Teilringes $k(\theta_0, \ldots, \theta_{n-1})$, und wegen

$$u^{p^{n-1}}\theta u^{-p^{n-1}} = \theta + \boldsymbol{p^{n-1}} \neq \theta, \quad u^{p^n}\theta u^{-p^n} = \theta + \boldsymbol{p^n} = \theta$$

hat dieser Automorphismus die Ordnung p^n.

Machen wir mit einer Zahl $\gamma \neq 0$ und einem Vektor δ aus k die simultanen Substitutionen

$$u' = \gamma u, \quad \alpha' = \alpha\gamma^{p^n}$$
$$\theta' = \theta + \delta, \quad \beta' = \beta + \wp\delta,$$

so gehen alle bisherigen Gleichungen in die entsprechenden Gleichungen für die gestrichenen Größen über. Daher gilt die Isomorphie

$$(\alpha, \beta] \cong (\alpha\gamma^{p^n}, \beta + \wp\delta]. \tag{22}$$

Satz 14. *Das eben erklärte System $(\alpha, \beta]$ ist einfach und normal und hat den Grad p^n.*

Beweis. Wir berufen uns auf einen allgemeinen Satz aus der Theorie hyperkomplexer Systeme: Ein System S über einem Körper k ist einfach und normal, wenn das mit dem algebraisch abgeschlossenen Körper $\bar{k}$ erweiterte System $\bar{S}$ einfach ist (und umgekehrt). Im Körper $\bar{k}$ haben wir aber wegen (22) mit $\gamma = \alpha^{p^{-n}}$ und $\delta = -\frac{1}{\wp}\beta$ die Isomorphie $(\alpha, \beta] \cong (1, 0]$. Wir müssen also zeigen, daß das System $(1, 0]$ einfach ist und den Rang p^{2n} hat.

Der kommutative Teilring $k(\theta_0, \ldots, \theta_{n-1})$ wird durch die Gleichungen $\theta^p - \theta = 0$, d. h. durch $\theta_i^p = \theta_i$ bestimmt, daher ist $k(\theta_0, \ldots, \theta_{n-1}) = \sum_1^{p^n} k\, e_i$ mit Idempotenten e_i. Die Transformation mit u liefert eine Permutation der e_i von der Ordnung p^n, also eine zyklische. Wir können somit den Ring $(1, 0]$ auch darstellen durch die Basis

$$e_\sigma u^\tau \ (\sigma, \tau \bmod p^n) \text{ vom Rang } p^{2n}$$

und die Rechenregeln

$$u^{p^n} = 1; \quad e_\sigma^2 = e_\sigma, \quad e_\sigma e_\tau = 0 \ \ (\sigma \neq \tau), \quad (\Sigma e_\sigma = 1), \quad u e_\sigma u^{-1} = e.$$

Im Ring $(1, 0]$ sei nun $\mathfrak{A}$ ein Ideal, das ein Element $A = \sum_{\sigma,\tau} a_{\sigma,\tau} e_\sigma u^\tau \neq 0$ enthält, es sei etwa $a_{s,t} \neq 0$. Eine leichte Rechnung ergibt

$$\sum_\varrho u^\varrho e_s a_{s,t}^{-1} A u^{-t} e_s u^{-\varrho} = 1,$$

also ist $\mathfrak{A} = (1)$, d. h. der Ring $(1, 0]$ ist einfach, w. z. b. w.

Nunmehr zeigen wir einige grundlegende Algebrenregeln:

Satz 15. *Es gilt* $(\alpha \mid 0, \beta_1, \ldots, \beta_{n-1}] \sim (\alpha \mid \beta_1, \ldots, \beta_{n-1}]$.

Beweis. Für den kommutativen Teilring $k(\theta_0, \ldots, \theta_{n-1})$ der linksstehenden Algebra L gilt

$$\wp(\theta_0, \theta_1, \ldots, \theta_{n-1}) = (0, \beta_1, \ldots, \beta_{n-1}),$$

also ist $\theta_0^p = \theta_0$. Wird die Gleichung $\wp(\theta_0, 0, \ldots, 0) = 0$ abgezogen, so bleibt

$$\wp(0, \theta_1, \ldots, \theta_{n-1}) = (0, \beta_1, \ldots, \beta_{n-1}),$$

also ist

$$(\alpha) \qquad \wp(\theta_1, \ldots, \theta_{n-1}) = (\beta_1, \ldots, \beta_{n-1}).$$

Aus

$$u^p(\theta_0, \theta_1, \ldots, \theta_{n-1})\, u^{-p} = (\theta_0, \theta_1, \ldots, \theta_{n-1}) + \boldsymbol{p}$$

folgt

$$(\beta) \qquad u^p(\theta_1, \ldots, \theta_{n-1})\, u^{-p} = (\theta_1, \ldots, \theta_{n-1}) + \mathbf{1}.$$

e_i ($i \bmod p$) seien die p Idempotente des Ringes $k(\theta_0)$, sie werden bei Transformation mit u zyklisch vertauscht, $ue_iu^{-1} = e_{i+1}$. Es gilt die Zerlegung

$$k(\theta_0, \ldots, \theta_{n-1}) = \sum_{i \bmod p} e_i k(\theta_1, \ldots, \theta_{n-1}),$$

also

$$L = \sum_i \sum_\nu e_i k(\theta_1, \ldots, \theta_{n-1})\, u^\nu,$$

folglich

$$e_0 L e_0 = \sum_{\nu \equiv 0 (p)} e_0 k(\theta_1, \ldots, \theta_{n-1})\, u^\nu.$$

Nach der hyperkomplexen Theorie ist $L \sim e_0 L e_0$. Der Ring $e_0 L e_0$ enthält e_0 als Einselement, er wird erzeugt von

$$e_0 u^p;\ e_0\theta_1, \ldots, e_0\theta_{n-1},$$

und nach (α), (β) bestehen die Relationen

$$(e_0u^p)^{p^{n-1}} = e_0\alpha,\ \ \wp(e_0\theta_1, \ldots, e_0\theta_{n-1}) = (e_0\beta_1, \ldots, e_0\beta_{n-1}),$$
$$e_0u^p \cdot (e_0\theta_1, \ldots, e_0\theta_{n-1}) \cdot e_0u^{-p} = (e_0\theta_1, \ldots, e_0\theta_{n-1}) + (e_0, \ldots, 0).$$

Da die rechtsstehende Algebra $R = (\alpha | \beta_1, \ldots, \beta_{n-1}]$ durch genau entsprechende Relationen definiert ist, ist die Isomorphie $e_0 L e_0 \cong R$ und damit die Ähnlichkeit $L \sim R$ nachgewiesen.

Wir können jetzt zeigen, daß jede Algebra $(\alpha, \beta]$ einer *zyklischen Algebra* ähnlich ist. Wenn nämlich $\beta_0 \neq \wp a$ ist, so ist nach Satz 13 $k\left(\frac{1}{\wp}\beta\right)$ ein zyklischer Körper vom Grad p^n, und mit dem dort angegebenen Automorphismus σ ist in der üblichen Schreibweise für zyklische Algebren offenbar

$$(\alpha, \beta] \sim \left(\alpha, k\left(\frac{1}{\wp}\beta\right), \sigma\right).$$

Ist dagegen $\beta_0 = \wp a$, so ist nach (20) $\beta \sim (0, \beta_1', \ldots, \beta_{n-1}')$, wegen (22) und Satz 15 ist also

$$(\alpha | \beta_0, \beta_1, \ldots, \beta_{n-1}] \sim (\alpha | 0, \beta_1', \ldots, \beta_{n-1}'] \sim (\alpha | \beta_1', \ldots, \beta_{n-1}'].$$

Wird diese Reduktionsmethode mehrfach angewandt, so kommen wir schließlich auf den vorhin behandelten Fall zurück, bzw. auf eine Algebra vom Rang 1.

Satz 16. *Es gelten die Regeln*

$$(\alpha, \beta] \cdot (\alpha', \beta] \sim (\alpha\alpha', \beta],$$
$$(\alpha, \beta] \cdot (\alpha, \beta'] \sim (\alpha, \beta + \beta'].$$

Beweis. Die Algebra $(\alpha, \beta] \cdot (\alpha', \beta']$ wird erzeugt von den Größen

$$\begin{cases} u, \theta & \text{mit } u^{p^n} = a, \quad \wp\theta = \beta, \quad u\theta u^{-1} = \theta + \mathbf{1}, \\ u', \theta' & \text{mit } u'^{p^n} = \alpha', \quad \wp\theta' = \beta', \quad u'\theta'u'^{-1} = \theta' + \mathbf{1}. \end{cases}$$

Dabei sind die Größen der ersten Zeile vertauschbar mit denen der zweiten.

Die Algebra wird aber auch erzeugt von den Größen

$$\begin{cases} v = uu', & \mathsf{H} = \theta \text{ mit } v^{p^n} = \alpha\alpha', \quad \wp\mathsf{H} = \beta, \quad v\mathsf{H}v^{-1} = \mathsf{H} + 1, \\ v' = u', & \mathsf{H}' = \theta' - \theta \text{ mit } v'^{p^n} = \alpha', \quad \mathsf{H}' = \beta' - \beta, v'\mathsf{H}'v'^{-1} = \mathsf{H}' + 1. \end{cases}$$

Dabei werden wieder die Größen der ersten Zeile vertauschbar mit denen der zweiten.

Infolgedessen gilt die Regel

$$(\alpha, \beta] \cdot (\alpha', \beta'] \sim (\alpha\alpha', \beta] \cdot (\alpha', \beta' - \beta].$$

Nun ist nach Satz 15 $(\alpha, 0] \sim 1$. Für $\beta = \beta'$ folgt daher die erste zu beweisende Regel $(\alpha, \beta] \cdot (\alpha', \beta] \sim (\alpha\alpha', \beta]$. Für $\alpha = 1$ ergibt sich hieraus $(1, \beta] \sim 1$. Setzen wir $\alpha' = \alpha^{-1}$ und $\beta' = 0$, so folgt $(\alpha, \beta] \sim (\alpha^{-1}, -\beta]$. Ersetzen wir die Größen α', β' durch α^{-1} und β', so erhalten wir die zweite zu beweisende Regel

$$(\alpha, \beta] \cdot (\alpha, \beta'] \sim (\alpha, \beta + \beta'].$$

7. Residuenformel für Algebren über einem Potenzreihenkörper.

In diesem Abschnitt sollen die Algebren $(\alpha, \beta]$ über einem speziellen Körper k untersucht werden.

C sei ein vollkommener Körper der Charakteristik p. Wir betrachten den Körper k aller Potenzreihen

$$\sum_{i>-\infty} c_i t^i, \qquad c_i \text{ aus } C.$$

Der im Abschnitt 2 eingeführte konstante Vektor (α, β) werde entsprechend auch für Vektoren β der Länge n eingeführt, so daß (α, β) ebenso lang wie β ist.

Satz 17. *Es besteht die* **Residuenformel** [3])

$$(\alpha\,|\,\beta] \sim (t\,|\,(\alpha, \beta)].$$

Beweis. Wir setzen den Quotienten $(\alpha\,|\,\beta] \cdot (t\,|\,(\alpha, \beta)]^{-1} = q(\alpha, \beta)$. Es gelten nach (9), (10) und Satz 16 die Regeln

$$(\alpha) \qquad q(\alpha\alpha', \beta) \sim q(\alpha, \beta) \cdot q(\alpha', \beta),$$

$$(\beta) \qquad q(\alpha, \beta + \beta') \sim q(\alpha, \beta) \cdot q(\alpha, \beta').$$

Enthalten alle Entwicklungen der β_ν nur Potenzen von t mit lauter positiven Exponenten, so konvergiert $\sum_0^\infty \beta^{p^h}$ komponentenweise gegen einen Vektor B. Wegen $\beta = \wp(-B)$ ist in diesem Fall $(t\,|\,\beta] \sim 1$.

Wenn alle Entwicklungen der β_ν nur Potenzen von t mit lauter negativen Exponenten enthalten, so ist ebenfalls $(t, \beta] \sim 1$, wie in einer nachfolgenden Arbeit von Teichmüller (dieser Bd. S. 141) bewiesen wird. (Dort wird benützt, daß C vollkommen ist.)

Zum Vektor β bilden wir wie im Beweis von Satz 4 die Vektoren β', β'' und $\Omega\beta = \beta - \beta' - \beta''$. Es folgt aus Satz 16 und den eben ausgeführten Tatsachen

$$(t\,|\,\Omega\beta] \sim (t\,|\,\beta] \cdot (t\,|\,\beta']^{-1} \cdot (t\,|\,\beta'']^{-1} \sim (t\,|\,\beta],$$

allgemeiner $(t\,|\,\beta] \sim (t\,|\,\Omega^n\beta]$. Es ist aber nach dem Beweis von Satz 4, weil wir es hier mit Vektoren der Länge n zu tun haben, $\Omega^n\beta = (t, \beta)$. Damit haben wir zunächst $q(t, \beta) \sim 1$ nachgewiesen.

---

[3]) Das sich für $p = 2$ ergebende Resultat

$$(t\,|\,\sum_i b_{0i} t^i, \sum_i b_{1i} t^i] \sim (t\,|\,b_{00}, b_{10} + \sum_{i>0} b_{0i} b_{0,-i}]$$

fand ich bereits im Januar 1935 durch sehr komplizierte nichtkommutative Rechnungen, bei denen nur das Ergebnis zufällig einfach erschien.

Nun sei $\alpha = a_m t^m + a_{m+1} t^{m+1} + \cdots (a_m \neq 0)$. Für die neue Variable $t' = t^{1-m}\alpha$ ist wieder $q(t', \beta) \sim 1$, folglich ist nach (α) und (β)

$$q(\alpha, \beta) \sim q(t, \beta)^{m-1} \cdot q(t', \beta) \sim 1, \text{ w. z. b. w.}$$

8. Berechnung der Invariante einer Algebra.

K_f sei der unverzweigte p-adische Körper mit dem Restklassenkörper C_f von p^f Elementen. k_f sei der Potenzreihenkörper mit C_f als Konstantenkörper. Derjenige Automorphismus von K_f, k_f bzw. C_f, der die Restklassen mod p, die Konstanten bzw. die Elemente in die p-te Potenz erhebt, werde einheitlich mit P bezeichnet. Ebenso soll die Spur über $K_f/K_1, k_f/k_1, C_f/C_1$ einheitlich mit Sp bezeichnet werden.

Über dem Körper k_f gibt es p^n verschiedene Algebren vom Grade p^n, die alle auf die zyklische Gestalt

$$(t^m, k_{nf}/k_f, P^f)$$

gebracht werden können, und welche durch die **Invariante** $\frac{m}{p^n}$ mod 1 charakterisiert werden. Wir wollen zeigen, wie die Invariante einer Algebra $(\alpha, \beta]$ berechnet werden kann.

Satz 18. *Es werde der Potenzreihe* $\alpha = \mathfrak{a}^m t_m + \mathfrak{a}_{m+1} t^{m+1} + \cdots$ *des Körpers* k_f *mit Koeffizienten* $\mathfrak{a}_\nu$ *aus dem Galoisfeld* C_f *eine Potenzreihe* $\mathsf{A} = A_m t^m + A_{m+1} t^{m+1} + \cdots$ *mit Koeffizienten* A_ν *aus dem p-adischen Körper* K_f *derart zugeordnet, daß* A_ν *in der Restklasse* $\mathfrak{a}_\nu$ mod p *liegt. Entsprechend werde komponentenweise auch dem Vektor* $(\beta_0, \ldots, \beta_{n-1})$ *ein Vektor* $(\mathsf{B}_0, \ldots, \mathsf{B}_{n-1})$ *zugeordnet.*

Die Invariante der Algebra

$$(\alpha \,|\, \beta_0, \ldots, \beta_{n-1}]$$

lautet dann

$$\operatorname{Sp} \operatorname{Res} \frac{d\mathsf{A}}{\mathsf{A}} \left(\frac{\mathsf{B}_0^{p^{n-1}}}{p^n} + \frac{\mathsf{B}_1^{p^{n-1}}}{p^{n-1}} + \cdots + \frac{\mathsf{B}_{n-1}}{p} \right) \text{ mod } 1.$$

Beweis. Wie in Satz 9 ordnen wir jedem Vektor $\mathfrak{x} = (\mathfrak{x}_0, \ldots, \mathfrak{x}_{n-1})$ mit Komponenten $\mathfrak{x}_\nu$ aus dem Galoisfeld C_f die Restklasse $\xi = \sum_0^{n-1} \mathfrak{x}_i^{p^{-i}} p^i$ mod p^n zu. Dabei soll $\mathfrak{x}_i^{p^{-i}}$ im multiplikativen Repräsentantensystem des Körpers K_f liegen und die Restklasse $\mathfrak{x}_i^{p^{-i}}$ mod p darstellen. Bei dieser additiven Zuordnung geht $P\mathfrak{x}$ über in $P\xi$, ebenso geht Sp $\mathfrak{x}$ über in Sp ξ.

Wir betrachten zunächst Algebren $(t, \mathfrak{x}]$ mit konstantem Vektor $\mathfrak{x}$. Wenn $(t, \mathfrak{x}]$ zerfällt, so ist t Norm einer Zahl des zyklischen unverzweigten Körpers $k_f\left(\frac{1}{\wp}\mathfrak{x}\right)/k_f$, daher ist der betreffende Körpergrad 1, und es ist $\mathfrak{x} = (P - 1)\mathfrak{y}$, also Sp $\mathfrak{x} = 0$. Deshalb werden die Algebren $(t, \mathfrak{x}]$ homomorph abgebildet auf Sp $\mathfrak{x}$. Ist umgekehrt Sp $\mathfrak{x} = 0$, so ist nach Satz 13 $\mathfrak{x} = (P - 1)\mathfrak{y}$, und die Algebra $(t, \mathfrak{x}]$ zerfällt. Die Abbildung der Algebren $(t, \mathfrak{x}]$ auf Sp $\mathfrak{x}$ bzw. auf Sp ξ mod p^n ist infolgedessen eine Isomorphie.

Damit ist gezeigt, daß die Invariante der Algebra $(t, \mathfrak{x}]$ gleich $\frac{c}{p^n}$ Sp ξ mod 1 ist, wobei die Restklasse c mod p^n nicht von $\mathfrak{x}$ abhängt:

$$(t, \mathfrak{x}] \sim (t^{c \operatorname{Sp} \xi}, k_{nf}/k_f, P^f).$$

Zur Berechnung von c wählen wir speziell einen Vektor $\mathfrak{x}$ mit $\operatorname{Sp}\mathfrak{x} = \mathbf{1}$, d. h. mit $\operatorname{Sp}\xi \equiv 1 \bmod p^n$. Die Algebra $(t, \mathfrak{x}]$ mit den Relationen

$$u^{p^n} = t, \quad (P - \mathbf{1})\theta = \mathfrak{x}, \quad u\theta u^{-1} = \theta + \mathbf{1}$$

hat dann den Exponenten p^n. Daher ist $k_f(\theta)/k_f$ ein unverzweigter Körper vom Grad p^n, also $k_f(\theta) = k_{nf}$. Wegen

$$(P^f - 1)\theta = \frac{P^f - 1}{P - 1}(P - 1)\theta = \frac{P^f - 1}{P - 1}\mathfrak{x} = \operatorname{Sp}\mathfrak{x} = \mathbf{1} \quad \text{oder} \quad P^f\theta = \theta + \mathbf{1}$$

können die Relationen für $(t, \mathfrak{x}]$ auch in der Form

$$u^{p^n} = t^1, \quad k_f(\theta) = k_{nf}, \quad u\theta u^{-1} = P^f\theta$$

geschrieben werden, dies sind aber gerade die Relationen für die Algebra $(t^1, k_{nf}/k_f, P^f)$. Damit ist $c \equiv 1 \bmod p^n$ nachgewiesen, und es ist allgemein gezeigt, daß die Algebra $(t, \mathfrak{x}]$ die Invariante $\frac{1}{p^n}\operatorname{Sp}\xi \bmod 1$ hat.

Aus der Restklasse $\mathfrak{x}_i \bmod p$ des Körpers K_f werde ein beliebiges Element X_i gewählt und der Vektor

$$X = (X_0, \ldots, X_{n-1} \mid X^{(0)}, \ldots, X^{(n-1)})$$

gebildet. Wird beachtet, daß für einen multiplikativen Repräsentanten r die Gleichung $\operatorname{Sp} r^p = \operatorname{Sp} r$ besteht, so folgt

$$\xi = \operatorname{Sp}\sum_0^{n-1} x_i^{p^{-i}} p^i = \operatorname{Sp}\sum_0^{n-1} x_i^{p^{n-i-1}} p^i \equiv \operatorname{Sp}\sum_0^{n-1} X_i^{p^{n-i-1}} p^i = \operatorname{Sp} X^{(n-1)} \bmod p^n.$$

Nun betrachten wir eine beliebige Algebra $(\alpha, \beta]$ und bilden gemäß Satz 18 A und B. Wird $\operatorname{Res}\frac{d\mathsf{A}}{\mathsf{A}}\mathsf{B}^{(i)} = X^{(i)}$ gesetzt und mit $\mathfrak{x}_i$ die Restklasse $X_i \bmod p$ bezeichnet, so ist nach Satz 17 $(\alpha, \beta] \cong (t, \mathfrak{x}]$. Die Invariante von $(\alpha, \beta]$ ist daher

$$\frac{1}{p^n}\operatorname{Sp} X^{(n-1)} = \frac{1}{p^n}\operatorname{Sp}\operatorname{Res}\frac{d\mathsf{A}}{\mathsf{A}}\mathsf{B}^{(n-1)} \bmod 1,$$

und dies war gerade zu beweisen.

9. Analogon zum Residuensatz.

Für einen algebraischen Funktionenkörper k der Charakteristik p mit vollkommenem Konstantenkörper teilen wir ohne Beweis noch folgendes mit:

Ist $\alpha \neq 0$ eine Zahl und β ein Vektor aus k, so werde an jeder Stelle $\mathfrak{p}$ der im Abschnitt 2 eingeführte Vektor (α, β) gebildet. Die Abhängigkeit von $\mathfrak{p}$ deuten wir durch einen Index an. Es gilt dann das Analogon zum Residuensatz

$$\sum_{\mathfrak{p}} (\alpha, \beta)_{\mathfrak{p}} = 0.$$

Der Beweis dieser Relation verläuft im Prinzip genau wie der übliche Beweis des Residuensatzes: Reduktion auf Geschlecht Null durch Spurbildung im Kleinen, und bei Geschlecht Null durch Zerlegung in Partialbrüche.

Die Relation $\sum_{\mathfrak{p}} = 0$ kann auch als Verallgemeinerung der Tatsache angesehen werden, daß die Summe der $\mathfrak{p}$-Invarianten einer Algebra $\equiv 0 \bmod 1$ ist.

Göttingen, 22. 6. 1936.

Eingegangen 29. August 1936.

Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper.

Von *Oswald Teichmüller* in Göttingen.

H. Hasse und F. K. Schmidt haben zuerst allgemeine Sätze über die Mannigfaltigkeit der verschiedenen Typen diskret bewerteter perfekter Körper aufgestellt [1]). Sie fanden als wichtigstes Bestimmungsstück dieser Körper den Restklassenkörper. Auf Grund des neuen Formalismus, den E. Witt veröffentlicht [2]) und dessen Zusammenhang mit der gewöhnlichen p-adischen Addition er auch selbst bemerkte, gelang es mir, die Ergebnisse von Hasse und F. K. Schmidt nicht nur auf übersichtlicherem Wege zu beweisen, sondern auch die Struktur von dort als vorhanden nachgewiesenen Körpern durch explizite Formeln festzulegen. Eine Skizze dieser Untersuchungen veröffentlichte ich bereits [3]); eine ausführlichere Darstellung an dieser Stelle sollte folgen.

Inzwischen hat aber Witt selbst die Hauptergebnisse (nämlich die Strukturuntersuchung der diskret bewerteten perfekten Körper mit vollkommenem Restklassenkörper von Primzahlcharakteristik) in seine eben zitierte Arbeit ohne wesentliche Abänderung aufgenommen. Deshalb kann ich mich darauf beschränken, hier den Fall eines unvollkommenen Restklassenkörpers auf jenen schon erledigten Fall zurückzuführen.

Der Vollständigkeit wegen werden gelegentlich auch wohlbekannte Hilfssätze bewiesen.

Ein *diskret bewerteter Körper* ist ein Körper K, in dem jedem Element α eine Zahl $w(\alpha)$ folgendermaßen zugeordnet ist:

$$(1) \qquad \begin{cases} w(0) = \infty, \quad w(\alpha) \text{ ganzrational für } \alpha \neq 0; \\ w(\alpha + \beta) \geqq \operatorname{Min}(w(\alpha),\ w(\beta)); \\ w(\alpha\beta) = w(\alpha) + w(\beta). \end{cases}$$

Wir dürfen, ohne interessante Fälle zu verlieren, annehmen, daß K ein Element π mit

$$w(\pi) = 1$$

enthält; jedes solche π heißt *Primelement*. Die Menge I aller $\alpha \in K$ mit $w(\alpha) \geqq 0$ ist ein Integritätsbereich, dessen Quotientenkörper K ist; I heißt der *Bewertungsring*. Die *Ideale* von I sind:

$$I = (1), \quad (\pi), \quad (\pi^2), \ldots, (0).$$

---

[1]) H. Hasse und F. K. Schmidt, Die Struktur diskret bewerteter Körper, dieses Journal **170** (1934).

[2]) E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, dieser Band, S. 126.

[3]) O. Teichmüller, Über die Struktur diskret bewerteter perfekter Körper, Gött. Nachrichten N. F. **1** (1936).

$\alpha \equiv \beta \pmod{\pi^n}$ ist gleichbedeutend mit $w(\alpha - \beta) \geqq n$. Der *Restklassenring* $I/(\pi^n)$ heiße $\mathfrak{R}_n$, die Elemente von $\mathfrak{R}_n$ sind also als Restklassen spezielle Teilmengen von I. Für $m < n$ ist jede Restklasse aus $\mathfrak{R}_n$ in einer Restklasse aus $\mathfrak{R}_m$ enthalten, und es gilt

$$\mathfrak{R}_n/(\pi^m) \cong \mathfrak{R}_m .$$

Besonders wichtig ist $\mathfrak{R}_1$; dieser Restklassenring ist sogar ein Körper $\mathfrak{K}$:

$$\mathfrak{K} = \mathfrak{R}_1 = I/(\pi) .$$

$\mathfrak{K}$ heißt der *Restklassenkörper* von K. All diese Bezeichnungen werden in der ganzen Arbeit angewandt.

K heißt *perfekt*, wenn es zu jeder Folge α_n aus K, für die $\lim w(\alpha_n - \alpha_m) = \infty$ gilt, ein $\alpha \in K$ mit $\lim w(\alpha_n - \alpha) = \infty$ gibt; dies α heißt dann $\lim \alpha_n$. Wir formen diese Bedingung um.

Hilfssatz 1. *K ist dann und nur dann perfekt, wenn I perfekt ist.*

Beweis. K sei perfekt, α_n sei eine Folge aus I mit $\lim w(\alpha_n - \alpha_m) = \infty$. Dann gibt es ein $\alpha \in K$ mit $\lim w(\alpha_n - \alpha) = \infty$. Nach (1) gilt

$$w(\alpha) \geqq \operatorname{Min}\,(w(\alpha - \alpha_n), w(\alpha_n));$$

aber $w(\alpha_n)$ ist $\geqq 0$ und $w(\alpha - \alpha_n)$ strebt gegen ∞, darum $w(\alpha) \geqq 0$, $\alpha \in I$.

Nun sei I perfekt, α_n sei eine Folge aus K mit $\lim w(\alpha_n - \alpha_m) = \infty$. Ist $w(\alpha_n - \alpha_N) \geqq 0$ für $n > N$, so ist

$$w(\alpha_n) \geqq \operatorname{Min}\,(0, w(\alpha_N)) \quad \text{für } n > N .$$

Daher gibt es ein M mit

$$w(\alpha_n) \geqq -M \quad \text{für alle } n .$$

$\pi^M \alpha_n$ ist dann eine Folge in I mit

$$w(\pi^M \alpha_n - \pi^M \alpha_m) = M + w(\alpha_n - \alpha_m) \to \infty ,$$

also gibt es ein $\beta \in I$ mit $\lim w(\pi^M \alpha_n - \beta) = \infty$; setzt man $\alpha = \beta \pi^{-M}$, so strebt

$$w(\alpha_n - \alpha) = w(\pi^M \alpha_n - \beta) - M \to \infty .$$

Unter einer *Restklassenschachtelung* verstehen wir eine Folge von Restklassen $\mathfrak{r}_1 \in \mathfrak{R}_1$, $\mathfrak{r}_2 \in \mathfrak{R}_2$, . . ., für die

$$\mathfrak{r}_1 > \mathfrak{r}_2 > \mathfrak{r}_3 > \cdots$$

gilt.

Hilfssatz 2. *Dann und nur dann ist I (also K) perfekt, wenn jede Restklassenschachtelung sich auf ein Element von I zusammenzieht, also einen nichtleeren Durchschnitt hat.*

Beweis. I sei perfekt, $\mathfrak{r}_1 > \mathfrak{r}_2 > \cdots$ sei eine Restklassenschachtelung. α_n sei irgendein Element von $\mathfrak{r}_n$. Für $m < n$ gilt dann $\alpha_m \in \mathfrak{r}_m$ und auch $\alpha_n \in \mathfrak{r}_n \subset \mathfrak{r}_m$, also $\alpha_m \equiv \alpha_n \pmod{\pi^m}$ oder $w(\alpha_n - \alpha_m) \geqq m$. Daher strebt $w(\alpha_n - \alpha_m) \to \infty$; es gibt einen $\lim \alpha_n = \alpha \in I$. Zu jedem n gibt es ein $N \geqq n$ mit $w(\alpha_N - \alpha) \geqq n$; aus $\alpha_N \in \mathfrak{r}_N \subseteqq \mathfrak{r}_n$ und $\alpha \equiv \alpha_N \pmod{\pi^n}$ folgt $\alpha \in \mathfrak{r}_n$. Unser α liegt also in allen $\mathfrak{r}_n$.

α ist das einzige Element von I mit dieser Eigenschaft; denn liegen α und β in allen $\mathfrak{r}_n$, so gilt für alle n

$$\alpha \equiv \beta \pmod{\pi^n}$$

oder $w(\alpha - \beta) \geqq n$, $w(\alpha - \beta) = \infty$, $\alpha = \beta$.

Nun werde vorausgesetzt, jede Restklassenschachtelung ziehe sich auf ein Element von I zusammen, und α_n sei eine Folge in I mit $\lim w(\alpha_m - \alpha_n) = \infty$. Dann gilt für jedes k zuletzt $w(\alpha_n - \alpha_m) \geqq k$, zuletzt sind also alle α_n kongruent mod π^k, die letzten α_n liegen in einer einzigen Restklasse $\mathfrak{r}_k$ mod π^k. Diese $\mathfrak{r}_k$ bilden offenbar eine Restklassenschachte-

lung, sie mögen sich auf α zusammenziehen. Dann liegt α für jedes k mit den letzten α_n in derselben Restklasse $\mathfrak{r}_k \pmod{\pi^k}$, zuletzt ist $w(\alpha_n - \alpha) \geqq k$. Das heißt aber $\lim w(\alpha_n - \alpha) = \infty$.

Von jetzt an ist K immer perfekt.

Unter einem *Repräsentantensystem* (genauer: Repräsentantensystem von $I \bmod (\pi)$) versteht man eine Teilmenge von I, die mit jeder Restklasse aus $\mathfrak{R}_1 = \mathfrak{k}$ genau ein Element, den „*Repräsentanten*" dieser Restklasse, gemein hat. Bekannt ist

Hilfssatz 3. *Ist π_n eine Folge mit $w(\pi_n) = n$ (z. B. $\pi_n = \pi^n$) und R ein Repräsentantensystem in K, so läßt sich jedes Element von K eindeutig in der Form*

$$\alpha = \sum_{n=w(\pi_n)}^{\infty} a_n \pi_n \qquad (a_n \in R)$$

darstellen. Insbesondere lassen sich die Elemente von I eindeutig in der Form

$$\alpha = \sum_{n=0}^{\infty} a_n \pi^n \qquad (a_n \in R)$$

darstellen.

Wir werden später gelegentlich einen Oberkörper $\overline{K}$ endlichen Grades n von K zu betrachten haben. Die „Bewertung" $w(\alpha)$ von K läßt sich auf eine und nur eine Weise zu einer Bewertung $\overline{w}(\mathsf{A})$ fortsetzen, die den Elementen A von $\overline{K}$ Zahlen so zuordnet, daß (1) gilt. Nur sind die Werte $\overline{w}(\mathsf{A})$ nicht mehr notwendig ganze Zahlen, sondern es können Brüche auftreten, die aber jedenfalls Vielfache von $\frac{1}{n}$ sind. Ist $\overline{w}(\Pi) = \frac{1}{e}$ der kleinste positive Wert von w, so ist e eine natürliche Zahl, die *Verzweigungsordnung* von $\overline{K}/K$. Man kann $\overline{w}(\mathsf{A})$ durch das stets ganzzahlige $e\overline{w}(\mathsf{A})$ ersetzen und alle vorigen Schlüsse durchführen. Der Restklassenkörper $\overline{\mathfrak{k}}$ von $\overline{K}$ ist ein endlicher Oberkörper von $\mathfrak{k}$, der Grad $(\overline{\mathfrak{k}} : \mathfrak{k})$ heißt *Restklassengrad*. Es gilt

Hilfssatz 4. *Der Grad von $\overline{K}$ über K ist das Produkt aus Restklassengrad und Verzweigungsordnung.*

Wir interessieren uns hier für den Fall, daß der Restklassenkörper $\mathfrak{k}$ des diskret bewerteten Körpers K die *Primzahlcharakteristik* p hat. K hat dann entweder auch die Charakteristik p (*charakteristikgleicher Fall*) oder die Charakteristik 0 (*charakteristikungleicher Fall*). Im letzteren Fall liegt p selbst, als Element von I angesehen, in (π) und hat daher eine positive Ordnungszahl

$$w(p) = s \geqq 1;$$

ist $s = 1$, d. h. ist p ein Primelement, so heißt K *unverzweigt*.

$\mathfrak{k}$ heißt bekanntlich *vollkommen*, wenn man in $\mathfrak{k}$ aus jedem Element von $\mathfrak{k}$ die p-te Wurzel ziehen kann. Die Bestimmung der Struktur von K bei vollkommenem $\mathfrak{k}$ ist bei Witt a. a. O. veröffentlicht. Ich gebe nur die für uns wichtigen Hauptergebnisse an.

Hilfssatz 5. *K enthält ein ausgezeichnetes Repräsentantensystem R, das multiplikative Repräsentantensystem, das durch jede einzelne der folgenden Eigenschaften eindeutig bestimmt ist:*

1) *Liegt α_n in der Restklasse $\mathfrak{a}^{p^{-n}} (\mathfrak{a} \in \mathfrak{k})$, so strebt $\alpha_n^{p^n}$ für $n \to \infty$ gegen den Repräsentanten a von $\mathfrak{a}$ in R.*

2) *Ist $a_{\overline{n}|}$ der Repräsentant von $\mathfrak{a}^{p^{-n}}$ in R, so gilt $a_{\overline{n+1}|}^{p} = a_{\overline{n}|}$.*

3) *Sind a, b, c die Repräsentanten von $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ in R und gilt $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$, dann gilt auch $ab = c$.*

Hat K die Charakteristik p, so ist R ein Unterkörper von K, und K ist der Potenzreihenkörper mit dem Konstantenkörper R: $K = R\{\pi\}$.

Hat K die Charakteristik 0 und ist K unverzweigt, so kann man nach Hilfssatz 3 die Elemente von I in „p-adische Reihen“

$$\alpha = \sum_{n=0}^{\infty} a_n p^n, \qquad a_n \in R,$$

nach dem multiplikativen Repräsentantensystem R entwickeln. Wir setzen

$$a_n^{p^n} = x_n \in R$$

und schreiben auch

$$a_n = x_n^{p^{-n}};$$

die p^n-te Wurzel ist zwar nicht notwendig eindeutig, aber *in* R gibt es nur eine p^n-te Wurzel aus einem Repräsentanten x_n, weil sich die p^n-te Wurzel im Restklassenkörper eindeutig ziehen läßt. Wir haben also eine Darstellung

$$\alpha = \sum_{n=0}^{\infty} x_n^{p^{-n}} p^n \qquad (x_n \in R). \tag{2}$$

Wenn man nun mehrere solche p-adische Reihen addiert, subtrahiert oder multipliziert und das Ergebnis wieder in eine p-adische Reihe (2) entwickelt, so hängen die Restklassen $\mathfrak{x}_n \pmod p$ der Koeffizienten x_n des Ergebnisses *ganzrational* von den Restklassen der Koeffizienten der ursprünglichen Reihen ab. Wir notieren den Fall, daß die algebraische Summe mehrerer Repräsentanten aus R gebildet wird:

Hilfssatz 6. *Ist K unverzweigt und $\mathfrak{K}$ vollkommen und R das multiplikative Repräsentantensystem in K, so kann man die algebraische Summe mehrerer Repräsentanten in eine p-adische Reihe entwickeln*:

$$a + a' + \cdots - b - b' - \cdots = \sum_{n=0}^{\infty} c_n p^n \qquad (a, b, c \in R),$$

und die Restklassen $\mathfrak{c}_n^{p^n}$ der $c_n^{p^n}$ drücken sich im Restklassenkörper $\mathfrak{K}$ ganzrational durch die Restklassen $\mathfrak{a}, \mathfrak{a}', \ldots, \mathfrak{b}, \mathfrak{b}', \ldots$ der $a, \ldots$ aus.

Ferner gilt

Hilfssatz 7. *Ist K charakteristikungleich bewertet und $\mathfrak{K}$ vollkommen, so enthält K einen einzigen unverzweigten Unterkörper K', der hinsichtlich derselben Bewertung perfekt ist und denselben Restklassenkörper $\mathfrak{K}$ wie K hat.*

„Denselben Restklassenkörper“, das heißt natürlich nicht nur, die Restklassenkörper von K und K' seien isomorph. Der Ausdruck ist vielmehr so zu verstehen: jedes Element des Restklassenkörpers $\mathfrak{K}'$ von K' liegt in einer und nur einer Restklasse aus $\mathfrak{K}$, und jede Restklasse aus $\mathfrak{K}$ enthält auch höchstens eine Restklasse aus $\mathfrak{K}'$. Man identifiziert die Restklassen aus $\mathfrak{K}'$ mit den sie enthaltenden Restklassen aus $\mathfrak{K}$ und macht so in eindeutig bestimmter Weise $\mathfrak{K}'$ zu einem Unterkörper von $\mathfrak{K}$. Dieser Unterkörper $\mathfrak{K}'$ von $\mathfrak{K}$ soll im vorliegenden Fall mit $\mathfrak{K}$ zusammenfallen.

Bevor wir in die eigentliche Strukturuntersuchung eintreten, noch ein Hilfssatz über das Rechnen mod p:

Hilfssatz 8. *Der Restklassenkörper $\mathfrak{K}$ habe die Charakteristik p. Für Elemente a, b aus I folgt aus $a \equiv b \pmod{\pi^n}$, daß $a^{p^r} \equiv b^{p^r} \pmod{\pi^{n+r}}$.*

Beweis. Ist $b = a + \pi^n c$, so ist

$$b^p = a^p + \binom{p}{1} a^{p-1}\pi^n c + \cdots + \binom{p}{p-1} a(\pi^n c)^{p-1} + (\pi^n c)^p .$$

Hierin sind die Binomialkoeffizienten durch p, also erst recht durch π teilbar (wegen $p \equiv 0 \pmod{\pi}$), die mittleren Glieder sind also durch π^{n+1} teilbar, während das letzte sogar durch π^{p^n} teilbar ist. Es bleibt

$$a^p \equiv b^p \pmod{\pi^{n+1}}.$$

Man mache Induktion nach r.

Durch die Hilfssätze 5 bis 7 wird die Struktur der diskret bewerteten perfekten Körper mit vollkommenem Restklassenkörper beschrieben. Wir nehmen nun an, K sei ein *diskret bewerteter perfekter Körper mit dem unvollkommenen Restklassenkörper* $\mathfrak{K}$ *der Charakteristik* p.

In einer anderen Arbeit [4]) skizzierte ich einen Beweis für

Hilfssatz 9. *$\mathfrak{K}$ hat eine p-Basis $\mathfrak{M}$, d. h. eine Teilmenge $\mathfrak{M}$ mit folgenden Eigenschaften:*

a) *Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ r verschiedene Elemente von $\mathfrak{M}$, so hat*

$$\mathfrak{K}\left(\sqrt[p]{\mathfrak{a}_1}, \ldots, \sqrt[p]{\mathfrak{a}_r}\right)$$

über $\mathfrak{K}$ den Grad p^r.

b) $\mathfrak{K}^p(\mathfrak{M}) = \mathfrak{K}$.

Wir wählen ein für alle Mal *eine feste p-Basis* $\mathfrak{M}$ von $\mathfrak{K}$ aus. Zwei Eigenschaften der p-Basis sollen gleich festgestellt werden:

Hilfssatz 10. *Sind m und n ganze Zahlen mit $m < n$, so gilt*

$$\mathfrak{K}^{p^n}(\mathfrak{M}^{p^m}) = \mathfrak{K}^{p^m}.$$

Beweis. Aus $\mathfrak{K}^p(\mathfrak{M}) = \mathfrak{K}$ folgt

$$\mathfrak{K}^{p^2}(\mathfrak{M}) = \mathfrak{K}^{p^2}(\mathfrak{M}^p)\,(\mathfrak{M}) = (\mathfrak{K}^p(\mathfrak{M}))^p\,(\mathfrak{M}) = \mathfrak{K}^p(\mathfrak{M}) = \mathfrak{K}$$

und genau so allgemein

$$\mathfrak{K}^{p^k}(\mathfrak{M}) = \mathfrak{K}.$$

Hieraus folgt

$$\mathfrak{K}^{p^k+m}(\mathfrak{M}^{p^m}) = \mathfrak{K}^{p^m} \qquad (k > 0).$$

Man muß nur beachten, daß bei Charakteristik p das Erheben eines Körpers in die p-te Potenz ein Isomorphismus ist.

Hilfssatz 11. *Die Ausdrücke*

$$\mathfrak{A} = \mathfrak{a}_1^{e_1} \cdots \mathfrak{a}_r^{e_r}, \tag{3}$$

worin $r \geqq 0$, $a_1, \ldots, a_r$ verschiedene Elemente von $\mathfrak{M}$, $0 < e_i \leqq p^n - 1$, bilden eine (lineare) Basis von $\mathfrak{K}$ über $\mathfrak{K}^{p^n}$.

Beweis. Nach Hilfssatz 10 ist $\mathfrak{K} = \mathfrak{K}^{p^n}(\mathfrak{M})$, jedes Element von $\mathfrak{K}$ liegt also in einem Körper $\mathfrak{K}^{p^n}(\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ $(\mathfrak{a}_i \in \mathfrak{M})$. Weil aber jedes $\mathfrak{a}_i$ einer Gleichung p^n-ten Grades über $\mathfrak{K}^{p^n}$ genügt, sind alle Elemente von $\mathfrak{K}^{p^n}(\mathfrak{a}_i)$ i. b. a. $\mathfrak{K}^{p^n}$ linear von den

$$\mathfrak{A} = \mathfrak{a}_1^{e_1} \cdots \mathfrak{a}_r^{e_r} \quad (0 \leqq e_i \leqq p^n - 1) \tag{4}$$

abhängig. Es bleibt zu zeigen, daß je endlich viele Ausdrücke (3) i. b. a. $\mathfrak{K}^{p^n}$ linear unabhängig sind; das tun wir, indem wir zeigen, daß die Ausdrücke (4) stets i. b. a. $\mathfrak{K}^{p^n}$

---

[4]) O. Teichmüller, p-Algebren, Deutsche Mathematik **1** (1936).

linear unabhängig sind, nämlich indem wir

$$(\mathfrak{K}^{p^n}(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) : \mathfrak{K}) = p^{nr}$$

beweisen.

Selbstverständlich ist $(\mathfrak{K}^{p^n}(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) : \mathfrak{K}) \leqq p^{nr}$, wir haben die umgekehrte Ungleichung zu beweisen. — Für $\nu = 1, \ldots, n$ wird sich der Grad

$$(\mathfrak{K}^{p^n}(\mathfrak{a}_i^{p^\nu}) : \mathfrak{K}^{p^n}(\mathfrak{a}_i^{p^{\nu-1}}))$$

nicht vergrößern, wenn man mit $\mathfrak{K}^{p^\nu}$ erweitert:

$$(\mathfrak{K}^{p^n}(\mathfrak{a}_i^{p^\nu}) : \mathfrak{K}^{p^n}(\mathfrak{a}_i^{p^{\nu-1}})) \geqq (\mathfrak{K}^{p^\nu} : \mathfrak{K}^{p^\nu}(\mathfrak{a}_i^{p^{\nu-1}})) = p^r$$

nach der Eigenschaft a) der p-Basis $\mathfrak{M}$. Durch Multiplikation über ν folgt die Behauptung.

Nun greifen wir aus jeder Restklasse $\mathfrak{a} \in \mathfrak{M}$ einen Vertreter a beliebig heraus; diese a bilden eine Menge M. Die Auswahl von M ist wie die einer p-Basis $\mathfrak{M}$ von $\mathfrak{K}$ recht willkürlich, wir halten aber in der ganzen folgenden Untersuchung an dem einmal gewählten M fest.

Hilfssatz 12. $w(a) = 0$ *für* $a \in M$.

Beweis. a liegt als Element einer Restklasse mod π in I, also $w(a) \geqq 0$. Wäre $w(a) > 0$, so wäre $a \equiv 0 \pmod{\pi}$, die Restklasse $\mathfrak{a}$ von a wäre 0. Die Restklasse 0 kann aber in einer p-Basis von $\mathfrak{K}$ (wegen a)) nicht vorkommen.

Hilfssatz 13. *$\overline{K}$ sei ein Oberkörper endlichen Grades von K von der Form*

$$\overline{K} = K(a_{1\overline{1}|}, \ldots, a_{r\overline{1}|}) \quad mit \quad a_{i\overline{1}|}^p = a_i,$$

wo die a_i r verschiedene Elemente von M sind. Dann hat $\overline{K}$ über K den Grad p^r, und wenn man die Bewertung w von K auf $\overline{K}$ überträgt, wird der Restklassengrad p^r und die Verzweigungsordnung 1. *Das auf $\overline{K}$ fortgesetzte w nimmt also auch in $\overline{K}$ von selbst (ohne vorherige Multiplikation mit einer Zahl e) ganzzahlige Werte an.*

Beweis. Selbstverständlich ist $(\overline{K} : K) \leqq p^r$. Nach Hilfssatz 4 ist also alles bewiesen, wenn gezeigt ist, daß der Restklassengrad von $\overline{K}$ über K mindestens p^r ist.

Nach Hilfssatz 12 ist

$$w(a_{i\overline{1}|}) = \frac{1}{p}\, w(a_i) = 0.$$

Im Restklassenkörper $\overline{\mathfrak{K}}$ von $\overline{K}$ sei $\mathfrak{a}_{i\overline{1}|}$ die Restklasse von $a_{i\overline{1}|}$ mod π. Dann ist $\mathfrak{a}_{i\overline{1}|}^p = \mathfrak{a}_i$, $\overline{\mathfrak{K}}$ enthält also den Körper

$$\mathfrak{K}(\mathfrak{a}_{1\overline{1}|}, \ldots, \mathfrak{a}_{r\overline{1}|}) = \mathfrak{K}\left(\sqrt[p]{\mathfrak{a}_1}, \ldots, \sqrt[p]{\mathfrak{a}_r}\right).$$

Dieser hat aber nach der Eigenschaft a) der p-Basis den Grad p^r über $\mathfrak{K}$.

Wir sehen gleichzeitig, daß der Restklassenkörper $\overline{\mathfrak{K}}$ von $\overline{K}$ genau $\mathfrak{K}\left(\sqrt[p]{\mathfrak{a}_1}, \ldots, \sqrt[p]{\mathfrak{a}_r}\right)$ ist.

Außerdem folgt, daß K durch die definierenden Relationen $a_{i\overline{1}|}^p = a_i$ schon eindeutig festgelegt ist.

Wir bilden jetzt *das Kompositum $\widetilde{K}$ aller der Körper $\overline{K}$ des Hilfssatzes* 13. K entsteht also aus K durch Adjunktion je eines $a_{\overline{1}|}$ mit $a_{\overline{1}|}^p = a$ für alle $a \in M$. Die Elemente von $\widetilde{K}$ sind endliche Summen $\Sigma \alpha_{i_1, \ldots, i_r} a_{1\overline{1}|}^{i_1} \cdots a_{r\overline{1}|}^{i_r}$ $(\alpha \in K)$ und als solche Elemente von jeweils passenden Körpern $\overline{K}$, hierdurch ist das Rechnen in $\widetilde{K}$ beschrieben. w läßt sich in jedes $\overline{K}$, also auch in $\widetilde{K}$ als ganzzahlige diskrete Bewertung mit den Eigenschaften (1) fortsetzen. Aber wenn $\mathfrak{M}$ unendlich sein sollte, ist $\widetilde{K}$ nicht perfekt.

Wir schließen $\widetilde{K}$ ab: Der kleinste perfekte Oberkörper von $\widetilde{K}$ heiße $K_{\overline{1}|}$. Der Restklassenkörper von $K_{\overline{1}|}$ heiße $\mathfrak{R}_{\overline{1}|}$. Jede Restklasse aus $\mathfrak{R}_{\overline{1}|}$ enthält ein Element eines $\bar{K}$, läßt sich also auch als (auf $K_{\overline{1}|}$ fortgesetzte) Restklasse aus $\overline{\mathfrak{R}}$ deuten und liegt als solche in einem $\mathfrak{R}\left(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_r}\right)$; darum ist nach b)

$$\mathfrak{R}_{\overline{1}|} = \mathfrak{R}\left(\sqrt[p]{\overline{\mathfrak{M}}}\right) = \sqrt[p]{\overline{\mathfrak{R}}}\,.$$

Weil $\mathfrak{M}$ eine p-Basis von $\mathfrak{R}$ ist, ist $\sqrt[p]{\overline{\mathfrak{M}}}$ eine p-Basis von $\mathfrak{R}_{\overline{1}|} = \sqrt[p]{\overline{\mathfrak{R}}}$. Die Menge aller $a_{\overline{1}|}$, die ja der Menge M aller a durch $a^p_{\overline{1}|} = a$ eineindeutig zugeordnet ist, heiße $M_{\overline{1}|}$. Dann kann man $M_{\overline{1}|}$ als Repräsentantensystem für die Restklassen aus $\mathfrak{M}_{\overline{1}|} = \sqrt[p]{\overline{\mathfrak{M}}}$ auffassen. Die Überlegungen und Konstruktionen, die wir eben mit K und M ausgeführt haben, können wir also auch mit $K_{\overline{1}|}$ und $M_{\overline{1}|}$ ausführen. Wir erhalten so einen Körper $K_{\overline{2}|}$, der aus $K_{\overline{1}|}$ durch Adjunktion von je einer Lösung $a_{\overline{2}|}$ der Gleichung $a^p_{\overline{2}|} = a_{\overline{1}|}$ für jedes $a_{\overline{1}|}$ und nachfolgendes Abschließen entsteht und auf den sich die Bewertung w ganzzahlig fortsetzt und der den Restklassenkörper $\mathfrak{R}_{\overline{2}|} = \sqrt[p^2]{\overline{\mathfrak{R}}}$ hat. In ihm sei $M_{\overline{2}|}$ die Menge der $a_{\overline{2}|}$ $(a \in M)$ usw.

Wir haben schließlich eine *Folge ineinandergeschachtelter perfekter Körper*

$$K < K_{\overline{1}|} < K_{\overline{2}|} < \ldots < K_{\overline{n}|} < \ldots,$$

die durch ein und dieselbe Funktion w diskret und ganzzahlig bewertet sind, so daß ein Primelement π von K zugleich in allen $K_{\overline{n}|}$ Primelement ist. Jedem $a \in M$ ist eine Folge $a_{\overline{n}|} \in K_{\overline{n}|}$ mit $a^p_{\overline{n+1}|} = a_{\overline{n}|}$ zugeordnet, für jedes n sei $M_{\overline{n}|}$ die Menge der $a_{\overline{n}|}$, $a \in M$. Der Restklassenkörper von $K_{\overline{n}|}$ ist $\mathfrak{R}_{\overline{n}|} = \sqrt[p^n]{\overline{\mathfrak{R}}}$.

Nun bilden wir *die Vereinigungsmenge $\widetilde{L}$ der Körperfolge $K_{\overline{n}|}$*. Auch $\widetilde{L}$ ist offenbar ein Körper: Je zwei Elemente von $\widetilde{L}$ sind in irgendeinem $K_{\overline{n}|}$ enthalten, in diesem berechnet man Summe, Produkt usw. $\widetilde{L}$ ist auch durch w diskret bewertet. Jetzt schließen wir noch $\widetilde{L}$ ab: der kleinste perfekte Oberkörper von $\widetilde{L}$ heiße L, sein Restklassenkörper $\mathfrak{L}$. Es ist ohne weiteres zu sehen, daß $\mathfrak{L}$ die Vereinigung der Restklassenkörper $\mathfrak{R}_{\overline{n}|} = \sqrt[p^n]{\overline{\mathfrak{R}}}$ von K_n ist. $\mathfrak{L}$ entsteht also aus $\mathfrak{R}$ durch Adjunktion sämtlicher Restklassen $\mathfrak{a}_{\overline{n}|}$ mit $\mathfrak{a}^{p^n}_{\overline{n}|} = \mathfrak{a}$ für alle n und alle $\mathfrak{a} \in \mathfrak{M}$.

Hilfssatz 14. *$\mathfrak{L}$ ist der kleinste vollkommene Oberkörper von $\mathfrak{R}$.*

Beweis. Jeder vollkommene Oberkörper von $\mathfrak{R}$ muß offenbar $\mathfrak{L}$ enthalten; wir müssen zeigen, daß $\mathfrak{L}$ vollkommen ist. Jedes Element von $\mathfrak{L}$ liegt in einem $\mathfrak{R}_{\overline{n}|}$, nach Hilfssatz 10 $(\mathfrak{R}^{p^{-n}}(\mathfrak{M}^{p^{-n-1}}) = \mathfrak{R}^{p^{-n-1}})$ liegt seine p-te Wurzel in $\mathfrak{R}_{\overline{n+1}|}$, also gleichfalls in $\mathfrak{L}$.

Wir werden jetzt unsere Kenntnisse über die Struktur des diskret bewerteten perfekten Körpers L mit dem vollkommenen Restklassenkörper $\mathfrak{L}$ der Charakteristik p anwenden und daraus Folgerungen in bezug auf K ziehen.

Zuerst habe K die Charakteristik p. Dann hat auch L die Charakteristik p. Das multiplikative Repräsentantensystem R für die Restklassen aus $\mathfrak{L}$ in L ist in diesem

Falle ein Körper. T sei das Teilsystem derjenigen Repräsentanten aus R, welche die Restklassen aus $\mathfrak{K}$ vertreten.

Hilfssatz 15. *T ist ein Körper.*

Beweis. Summen, Differenzen, Produkte und Quotienten von T-Elementen liegen im Körper R und ihre Restklassen mod π liegen in $\mathfrak{K}$.

Hilfssatz 16. *$T \subset K$.*

Beweis. $\mathfrak{a}$ sei ein Element von $\mathfrak{K}$. Dann liegt $\sqrt[p^n]{\mathfrak{a}}$ in $\sqrt[p^n]{\mathfrak{K}} = \mathfrak{K}_{\overline{n}|}$, enthält also ein Element α_n aus $K_{\overline{n}|}$. Weil $K_{\overline{n}|}$ aus K durch Adjunktion gewisser p^n-ter Wurzeln und nachfolgendes Abschließen entstanden ist, kann man die p^n-te Potenz eines jeden Elements von $\mathfrak{K}_{\overline{n}|}$, auch $\alpha_n^{p^n}$, durch Elemente von K approximieren; weil K perfekt ist, folgt $\alpha_n^{p^n} \in K$. Nach Hilfssatz 5 strebt aber $\alpha_n^{p^n}$ für $n \to \infty$ gegen den R-Repräsentanten der Restklasse $\mathfrak{a}$, auch dieser liegt also in K.

Wir haben also innerhalb des Ausgangskörpers K ein Repräsentantensystem T gefunden, das ein Körper ist. Nach Hilfssatz 3 lassen sich die Elemente von K eindeutig in die Form

$$\alpha = \sum a_n \pi^n \qquad (a \in T) \tag{5}$$

bringen. Wenn man zwei derartige Reihen nach den gewöhnlichen Potenzreihenrechenregeln addiert oder multipliziert, erhält man immer wieder eine Potenzreihe der gleichen Form (5). Mit dieser Feststellung ist die Struktur von K genau beschrieben:

K ist der (in üblicher Weise bewertete) Potenzreihenkörper über einem zu $\mathfrak{K}$ isomorphen Teilkörper T.

Als Entwicklungsgröße kann man ein beliebiges Primelement π nehmen.

Wir kommen jetzt zum *charakteristikungleichen Fall* und untersuchen erst *unverzweigte Körper*. K sei also ein diskret bewerteter perfekter Körper der Charakteristik 0 mit dem unvollkommenen Restklassenkörper $\mathfrak{K}$ der Charakteristik p, und p sei ein Primelement von K.

Wir werden für alle $n = 0, 1, 2, \ldots$ den *Restklassenring*

$$\mathfrak{R}_{n+1} = I/(p^{n+1}),$$

wo I der Bewertungsring von K ist, als Unterring des entsprechenden Restklassenringes, den man für L bilden kann, beschreiben. Wir geben also diejenigen Restklassen aus $J/(p^{n+1})$ an, die ein Element aus I enthalten und die darum, wenn man in nun schon geläufiger Weise $I/(p^{n+1})$ als Unterring von $J/(p^{n+1})$ auffaßt, Elemente von $\mathfrak{R}_{n+1}$ werden; J bezeichnet natürlich den Bewertungsring von L.

Wir bemerken vorweg: aus $\alpha \equiv \beta \pmod p$ folgt nach Hilfssatz 8

$$\alpha^{p^{n-\nu}} \equiv \beta^{p^{n-\nu}} \pmod{p^{n-\nu+1}},$$

also

$$p^\nu \alpha^{p^{n-\nu}} \equiv p^\nu \beta^{p^{n-\nu}} \pmod{p^{n+1}}.$$

Eine Restklasse $\alpha \bmod p$ legt also eindeutig eine Restklasse $p^\nu \alpha^{p^{n-\nu}} \bmod p^{n+1}$ fest. Das gilt für $\nu = 0, 1, \ldots, n$.

Hilfssatz 17. *B sei (vgl. (3)) die Menge aller Ausdrücke*

$$A = a_1^{e_1} \cdots a_r^{e_r}, \tag{6}$$

worin $a_1, \ldots, a_r$ verschiedene Elemente von M und die $e_i \geqq 0$ sind.

Dann besteht $\mathfrak{R}_{n+1}$ genau aus allen Restklassen

$$\sum_i A_{i,0} x_{i,0}^{p^n} + p \sum_i A_{i,1} x_{i,1}^{p^{n-1}} + \cdots + p^\nu \sum_i A_{i,\nu} x_{i,\nu}^{p^{n-\nu}} + \cdots + p^n \sum_i A_{i,n} x_{i,n} \pmod{p^{n+1}}, \tag{7}$$

wo die $A_{i,\nu}$ aus B und die $x_{i,\nu} \in J$ Vertreter von Restklassen aus $\mathfrak{k}$ (z. B. die multiplikativen Repräsentanten dieser Restklassen mod p) *sind.*

Beweis. Wie schon oben bemerkt wurde, macht es nichts aus, wenn man die $x_{i,\nu}$ durch Elemente von I, die ihnen mod p kongruent sind, ersetzt. Dann stellt aber (7) ein Element von I dar. Wir müssen noch zeigen, daß jedes Element von I einem Ausdruck (7) mod p^{n+1} kongruent ist.

Nach Hilfssatz 11 ist jedes Element α von I einer Summe $\sum_i A_{i,0} x_{i,0}^{p^n}$ mod p kongruent, indem die Ausdrücke (6) mod p eine Basis von $\mathfrak{k}$ über $\mathfrak{k}^{p^n}$ enthalten. Die $x_{i,0}$ sollen Elemente von I sein. Aber

$$\beta = \frac{\alpha - \sum_i A_{i,0} x_{i,0}^{p^n}}{p} \tag{8}$$

liegt wieder in I, wir dürfen annehmen, β habe schon eine Darstellung

$$\beta \equiv \sum_i A_{i,1} x_{i,1}^{p^{n-1}} + \cdots + p^{\nu-1} \sum_i A_{i,\nu} x_{i,\nu}^{p^{n-\nu}} + \cdots + p^{n-1} \sum_i A_{i,n} x_{i,n} \pmod{p^n}. \tag{9}$$

Denn dieser Ausdruck geht aus (7) hervor, wenn man n durch $n-1$ ersetzt. Nun setzt man (9) in (8) ein und erhält (7).

Damit haben wir $\mathfrak{R}_{n+1}$ als Unterring von $J/(p^{n+1})$ ausgedrückt. In die Beschreibung (7) ging (außer L) nur der Restklassenkörper $\mathfrak{k}$ von K und die Menge M ein. M kann aber in L durch die p-Basis $\mathfrak{M}$ von $\mathfrak{k}$ charakterisiert werden:

Hilfssatz 18. *Die $a \in M$ sind in L die multiplikativen Repräsentanten ihrer Restklassen $\mathfrak{a} \in \mathfrak{M}$.*

Beweis. Wie schon bei der Konstruktion von L bemerkt wurde, gibt es zu jedem $a \in M$ eine Folge $a_{\overline{n}|}$ mit $a_{\overline{n+1}|}^{p} = a_{\overline{n}|}$. $a_{\overline{n}|}$ liegt also in der Restklasse $\mathfrak{a}^{p^{-n}}$, und es gilt $\lim_{n\to\infty} a_{\overline{n}|}^{p^n} = a$. Nach Hilfssatz 5 folgt die Behauptung.

Die $\mathfrak{R}_{n+1}$ sind also in $J/(p^{n+1})$ durch $\mathfrak{k}$ und durch $\mathfrak{M}$ eindeutig bestimmt.

Aber K ist durch die Gesamtheit der $\mathfrak{R}_{n+1}$ eindeutig als Unterkörper von L bestimmt. Denn K ist der Quotientenkörper von I, I ist aber, weil K perfekt ist, nach Hilfssatz 2 genau die Menge derjenigen $\alpha \in J$, die für jedes n in einer Restklasse aus $\mathfrak{R}_{n+1}$ liegen.

Hieraus folgt: *K ist durch $\mathfrak{k}$ bis auf Isomorphie eindeutig bestimmt.*

Denn ist auch K^* ein diskret bewerteter perfekter unverzweigter Körper der Charakteristik 0 mit dem Restklassenkörper $\mathfrak{k}^* \cong \mathfrak{k}$, so sei $\mathfrak{M}^*$ diejenige p-Basis von $\mathfrak{k}^*$, die $\mathfrak{M}$ bei dem gegebenen Isomorphismus $\mathfrak{k}^* \cong \mathfrak{k}$ entspricht, und M^* in K^* ein Repräsentantensystem für diese Restklassen. Wir konstruieren L^* wie vorher L; wegen $\mathfrak{L}^* \cong \mathfrak{L}$ besteht ein zugehöriger Isomorphismus $L^* \cong L$, denn das Rechnen in L ist durch das Rechnen in $\mathfrak{L}$ bestimmt. Dieser Isomorphismus läßt $\mathfrak{k}^*$ und $\mathfrak{k}$ sowie $\mathfrak{M}^*$ und $\mathfrak{M}$, mithin auch $\mathfrak{R}_{n+1}^*$ und $\mathfrak{R}_{n+1}$ sowie K^* und K einander entsprechen.

Wir haben auch eine Methode kennengelernt, um den unverzweigten Körper K zum Restklassenkörper $\mathfrak{k}$ zu konstruieren: Man bildet den kleinsten vollkommenen Oberkörper $\mathfrak{L}$ von $\mathfrak{k}$, konstruiert dazu den diskret bewerteten perfekten unverzweigten Körper L mit dem Restklassenkörper $\mathfrak{L}$, setzt für M die Menge der multiplikativen Repräsentanten einer p-Basis $\mathfrak{M}$ von $\mathfrak{k}$, bildet die Mengen $\mathfrak{R}_{n+1}$ nach der Formel (7), setzt I gleich der Menge aller α, die für jedes n in einer Restklasse aus $\mathfrak{R}_{n+1}$ mod p^{n+1} liegen und bildet K als Quotientenkörper von I. Wir werden bald noch genauer auf diese Konstruktion eingehen und werden beweisen, daß sie tatsächlich zu jedem $\mathfrak{k}$ einen diskret bewerteten perfekten unverzweigten Körper K der Charakteristik 0 mit dem vorgegebenen Restklassenkörper $\mathfrak{k}$ der Charakteristik p liefert.

Nehmen wir das einmal als richtig an. Dann können wir Hilfssatz 7 zum Teil auf unvollkommene Restklassenkörper übertragen:

In jedem diskret bewerteten perfekten Körper K der Charakteristik 0 mit dem unvollkommenen Restklassenkörper $\mathfrak{K}$ der Charakteristik p gibt es einen diskret bewerteten perfekten unverzweigten Teilkörper K' mit demselben Restklassenkörper $\mathfrak{K}$.

Wir bilden nämlich einfach zu K den Körper L, in diesem gibt es nach Hilfssatz 7 einen unverzweigten Unterkörper L' mit dem Restklassenkörper $\mathfrak{L}$. Wir wollten annehmen, es gebe zum Restklassenkörper $\mathfrak{K}$ schon einen diskret bewerteten perfekten unverzweigten Körper K'. Wir betten dann, von derselben p-Basis $\mathfrak{M}$ ausgehend wie bei der Konstruktion von L, K' in einen diskret bewerteten perfekten Körper mit dem Restklassenkörper $\mathfrak{L}$ ein; dieser muß zu L' (analytisch) isomorph sein, wir dürfen K' also gleich als Unterkörper von L' annehmen. Innerhalb L fallen dann natürlich die Restklassen mod π von K und von K' zusammen, und die Menge M der multiplikativen Repräsentanten der p-Basis $\mathfrak{M}$ von $\mathfrak{K}$ liegt schon in K'. Wir haben zu zeigen, daß K' ein Unterkörper von K ist.

Dazu stellen wir eine Erweiterung von Hilfssatz 17 auf. Es genügt nämlich zu zeigen, daß jedes Element α von K' mit $w(\alpha) \geqq 0$ stets mod $p^n\pi$ einem K-Element kongruent ist.

Wir wenden Hilfssatz 11 an, in dem wir aber n durch ns ersetzen ($s = w(p)$). Dann erhalten wir für α eine Darstellung

$$\alpha \equiv \sum_i A_{i,0}\, x_{i,0}^{p^{ns}} \pmod{p},$$

worin die A dieselbe Bedeutung wie in (6) haben und auch die x beliebige Repräsentanten von $\mathfrak{K}$-Restklassen in K' sind. Nun schreiben wir

$$\alpha = \sum_i A_{i,0} x_{i,0}^{p^{ns}} + p\beta$$

und wenden auf β denselben Schluß an usw. Ähnlich wie in Hilfssatz 17 entsteht

$$\alpha \equiv \sum_i A_{i,0}\, x_{i,0}^{p^{ns}} + p \sum_i A_{i,1}\, x_{i,1}^{p^{(n-1)s}} + \cdots + p^\nu \sum_i A_{i,\nu}\, x_{i,\nu}^{p^{(n-\nu)s}} + \cdots + p^n \sum_i A_{i,n}\, x_{i,n} \pmod{p^{n+1}},$$

erst recht mod $p^n\pi$. Die A liegen aber nicht nur in K', sondern auch in K, und die x vertreten Restklassen mod π aus $\mathfrak{K}$, dürfen also durch Vertreter derselben Restklassen, welche in K liegen, ersetzt werden. Denn ändert man x mod π ab, so ändert man $p^\nu x^{p^{(n-\nu)s}}$ höchstens mod $p^n\pi$ ab (nach Hilfssatz 8; vgl. die Bemerkung vor Hilfssatz 17). α ist also für alle n kongruent einem K-Element mod $p^n\pi$, eine Folge von Restklassen aus den Restklassenringen $\mathfrak{R}_{ns+1} = I/(p^n\pi)$ zieht sich auf α zusammen, darum muß α in K liegen. Jedes Element von K' ist aber der Quotient zweier α mit $w(\alpha) \geqq 0$, daher $K' \leqq K$, w. z. b. w.

Jetzt wenden wir uns endgültig wieder den unverzweigten Körpern zu und *beweisen, daß man wirklich nach der oben angegebenen Vorschrift zu jedem gegebenen unvollkommenen Restklassenkörper $\mathfrak{K}$ einen diskret bewerteten perfekten unverzweigten Körper der Charakteristik 0 mit dem vorgegebenen Restklassenkörper finden kann.*

$\mathfrak{K}$ sei also ein unvollkommener Körper der Charakteristik p. $\mathfrak{M}$ sei eine p-Basis von $\mathfrak{K}$, $\mathfrak{L}$ sei der kleinste vollkommene Oberkörper von $\mathfrak{K}$. L sei *der* diskret bewertete perfekte unverzweigte Körper mit dem Restklassenkörper $\mathfrak{L}$. R sei das multiplikative Repräsentantensystem in L, M sei die Menge der R-Repräsentanten der Elemente von $\mathfrak{M}$. J sei der Bewertungsring von L.

Für alle $n = 0, 1, 2, \ldots$ bilden wir als Teilmenge von $J/(p^{n+1})$ die Menge $\mathfrak{R}_{n+1}$ aller Restklassen

$$(10)\quad \sum_i \pm A_{i,0}\, x_{i,n}^{p^n} + \cdots + p^\nu \sum_i \pm A_{i,\nu}\, x_{i,\nu}^{p^{n-\nu}} + \cdots + p^n \sum_i \pm A_{i,n}\, x_{i,n} \pmod{p^{n+1}}.$$

Die A haben dieselbe Bedeutung wie in (6):

$$A = \prod_k a_k^{e_k}, \quad a_k \in M .$$

Die x sollen auch wie in (7) Vertreter von Restklassen aus $\mathfrak{K}$ sein, auf die Auswahl dieser Vertreter kommt es, wie schon vor Hilfssatz 17 bemerkt wurde, nicht weiter an, denn wir betrachten (10) ja nur mod p^{n+1}. Der einzige Unterschied zwischen (7) und (10) besteht darin, daß in (10) auch abwechselnde Vorzeichen zugelassen sind, das vereinfacht die nachfolgenden Überlegungen.

Man sieht ohne weiteres:

Hilfssatz 19. *$\mathfrak{R}_{n+1}$ ist ein Ring, und zwar derjenige Unterring von $J/(p^{n+1})$, der von den Restklassen a* (mod p^{n+1}) *und $p^\nu x^{p^{n-\nu}}$* (mod p^{n+1}) *erzeugt wird. a durchläuft hierin M, ν läuft von 0 bis n und x durchläuft ein Repräsentantensystem der Restklassen aus $\mathfrak{K}$.*

Zum Beweis hat man sich nur klar zu machen, daß auch ein Produkt $p^\nu x^{p^{n-\nu}} \cdot p^\mu y^{p^{n-\mu}}$ wieder in der Form (10) geschrieben werden kann: Für $\nu + \mu \leqq n$ ist

$$p^\nu x^{p^{n-\nu}} \cdot p^\mu y^{p^{n-\mu}} = p^{\nu+\mu} (x^{p^\mu} y^{p^\nu})^{p^{n-\nu-\mu}} ,$$

für $\nu + \mu > n$ ist

$$p^\nu x^{p^{n-\nu}} \cdot p^\mu y^{p^{n-\mu}} \equiv 0 \pmod{p^{n+1}} .$$

Noch trivialer ist

Hilfssatz 20. $\mathfrak{R}_1 = \mathfrak{K}$.

Hilfssatz 21. *Jede Restklasse aus $\mathfrak{R}_{n+1}$ enthält mindestens eine Restklasse aus $\mathfrak{R}_{n+2}$.*

Beweis. Nach Hilfssatz 19 braucht bloß bewiesen zu werden, daß jedes $p^\nu x^{p^{n-\nu}}$ mod p^{n+1} kongruent ist einem Ausdruck der Form (10), in dem n durch $n+1$ ersetzt ist.

Nach Hilfssatz 11 ist

$$x \equiv \sum_{k=1}^{g} A_k \, y_k^{p^{n+1}} \pmod{p} ,$$

worin A wie in (6) und die y Repräsentanten von $\mathfrak{K}$-Restklassen sind. Wir erheben die Kongruenz in die $p^{n-\nu}$-te Potenz und erhalten nach Hilfssatz 8

$$p^\nu x^{p^{n-\nu}} \equiv p^\nu \sum_{i_1 + \cdots + i_g = p^{n-\nu}} \frac{p^{n-\nu}!}{i_1! \cdots i_g!} (A_1 y_1^{p^{n+1}})^{i_1} \cdots (A_g y_g^{p^{n+1}})^{i_g} \pmod{p^{n+1}} .$$

Hier liegt tatsächlich auf der rechten Seite jeder Summand, mod p^{n+2} betrachtet, in dem von den Restklassen $a \in M$ und den Restklassen $p^\nu y^{p^{n-\nu+1}}$ (y mod p Repräsentant einer $\mathfrak{K}$-Restklasse) mod p^{n+2} erzeugten Ring $\mathfrak{R}_{n+2}$.

Nun kommt ein schwererer Hilfssatz, der ein eigentümliches Licht auf den Mechanismus der p-adischen Addition wirft. Er nützt die Eigenschaft a) der p-Basis $\mathfrak{M}$ aus, während in Hilfssatz 21 die Eigenschaft b) benützt wurde.

Hilfssatz 22. *Jede durch p teilbare Restklasse aus $\mathfrak{R}_{n+1}$ entsteht durch Multiplikation von p mit einer Restklasse aus $\mathfrak{R}_n$.*

Beweis. In (10) liegen offenbar alle Ausdrücke in $p\,\mathfrak{R}_n$ außer $\sum_i \pm A_i x_i^{p^n}$ (ich lasse den Index 0 jetzt weg). Hierin können wir die

$$A_i = a_1^{e_{1,i}} \cdots a_r^{e_{r,i}} \qquad (a \in M)$$

offenbar auf

$$0 \leqq e_{\varrho,i} \leqq p^n - 1$$

normieren, weil man die p^n-te Potenz eines a mit in das $x_i^{p^n}$ stecken kann. Nehmen wir nun an, es sei

$$\sum_i \pm A_i x_i^{p^n} \equiv 0 \pmod{p} .$$

Weil die normierten A nach Hilfssatz 11 mod p eine Basis von $\mathfrak{R}^{p^n}$ über $\mathfrak{R}$ bilden, muß für jedes einzelne A die über die zugehörigen x_i erstreckte algebraische Summe $\sum_i \pm x_i^{p^n}$ für sich $\equiv 0 \pmod p$ sein. Wir zeigen, daß dann $\sum_i \pm x_i^{p^n}$ mod p^{n+1} in $p\mathfrak{R}_n$ liegt.

Die x_i waren ursprünglich beliebige Repräsentanten ihrer in $\mathfrak{R}$ liegenden Restklassen, wir ersetzen sie jetzt durch Repräsentanten aus dem multiplikativen Repräsentantensystem R (das ist erlaubt). Nach Hilfssatz 6 ist

$$\sum_i \pm x_i^{p^n} = \sum_{\nu=0}^{\infty} c_\nu p^\nu, \qquad c_\nu \in R, \tag{11}$$

wo die Restklassen $\mathfrak{c}_\nu^{p^\nu}$ mod p der $c_\nu^{p^\nu}$ sich ganzrational aus den Restklassen $\mathfrak{x}_i^{p^n}$ der $x_i^{p^n}$ berechnen lassen. Die $\mathfrak{x}_i$ lagen in $\mathfrak{R}$, die $\mathfrak{x}_i^{p^n}$ demnach in $\mathfrak{R}^{p^n}$; darum müssen auch die $\mathfrak{c}_\nu^{p^\nu}$ in $\mathfrak{R}^{p^n}$ liegn, d. h. $\mathfrak{c}_\nu \in \mathfrak{R}^{p^{n-\nu}}$.

Nach Voraussetzung ist $\sum_i \pm x_i^{p^n} \equiv c_0 \equiv 0 \pmod p$, also wegen $c_\nu \in R$

$$c_0 = 0.$$

Setzt man noch

$$c_\nu = y_\nu^{p^{n-\nu}}, \qquad y_\nu \in R \qquad (\nu = 1, \ldots, n),$$

so sind die y_ν Vertreter von Restklassen aus $\mathfrak{R}$, und (11) geht über in

$$\sum_i \pm x_i^{p^n} \equiv p y_1^{p^{n-1}} + \cdots + p^n y_n \pmod{p^{n+1}}.$$

Damit ist gezeigt, daß $\sum_i \pm x_i^{p^n}$ mod p^{n+1} in einer mit p multiplizierten $\mathfrak{R}_n$-Restklasse liegt.

Diese Hilfssätze ermöglichen uns nun die Konstruktion des gesuchten Unterkörpers K von L.

Jede Restklassenschachtelung

$$\mathfrak{r}_1 > \mathfrak{r}_2 > \cdots, \quad \mathfrak{r}_n \in \mathfrak{R}_n,$$

zieht sich nach Hilfssatz 2 auf ein Element von J zusammen, die Gesamtheit der so erhaltenen Elemente heiße I. Weil nach Hilfssatz 19 alle $\mathfrak{R}_n$ Ringe sind, ist offenbar auch I ein Ring. Ist $\mathfrak{a}$ eine beliebige Restklasse aus $\mathfrak{R}$, so liegt sie nach Hilfssatz 20 in $\mathfrak{R}_1$, nach Hilfssatz 21 enthält sie eine Restklasse aus $\mathfrak{R}_2$, diese enthält wieder eine Restklasse aus $\mathfrak{R}_3$ usf.; diese Folge zieht sich auf ein Element von I zusammen. Jede Restklasse aus $\mathfrak{R}$ enthält also ein Element aus I. Umgekehrt ist nach Hilfssatz 20 klar, daß jedes Element aus I mod p in einer Restklasse aus $\mathfrak{R}$ liegt. Wie in Hilfssatz 2 sieht man, daß I perfekt ist.

K sei der Quotientenkörper von I. K ist als Unterkörper von L selbstverständlich ein diskret bewerteter Körper der Charakteristik 0, in dem p ein Primelement ist. Wir werden gleich zeigen, *daß jedes Element $\vartheta \in K$ mit $w(\vartheta) \geqq 0$ in I liegt.* Nach Hilfssatz 1 ist dann K perfekt, und wie soeben festgestellt wurde ist der Restklassenkörper dann $\mathfrak{R}$.

Jedes Element ϑ von K hat die Form $\frac{\alpha}{\beta}$; $\alpha, \beta \in I$. Ist $w(\alpha) = a$, $w(\beta) = b$, so ist nach Hilfssatz 22 $\alpha = p^a \alpha'$, $\beta = p^b \beta'$; $\alpha', \beta' \in I$. Es sei $w\left(\frac{\alpha}{\beta}\right) \geqq 0$, dann ist $a \geqq b$. Die Restklasse β' mod p, also auch ihr Reziprokes liegen in $\mathfrak{R}$, darum gibt es ein $\gamma \in I$ mit $\beta'\gamma \equiv 1 \pmod p$. Es sei

$$\beta'\gamma = 1 - \delta, \qquad \delta \in I, \qquad w(\delta) > 0.$$

Dann ist

$$\frac{\alpha}{\beta} = p^{a-b} \alpha' \gamma (1 + \delta + \delta^2 + \cdots) \in I.$$

Eingegangen 5. September 1936.

Schiefkörper über diskret bewerteten Körpern.

Von *Ernst Witt* in Göttingen.

Der diskret bewertete perfekte Körper k habe den vollkommenen Restklassenkörper $\mathfrak{k}$ mit beliebiger Charakteristik.

Die endlichen Körper $\mathfrak{K}/\mathfrak{k}$ einerseits und die endlichen unverzweigten Körper K/k mit Restklassenkörper $\mathfrak{K}/\mathfrak{k}$ andererseits entsprechen sich gegenseitig. Mit dem einem ist auch der andere Körper galoissch, und zwar induziert die galoissche Gruppe von K/k diejenige von $\mathfrak{K}/\mathfrak{k}$. Dies sind bekannte Tatsachen aus der Theorie der diskret bewerteten perfekten Körper.

Wir wollen hier zeigen, daß entsprechende Tatsachen auch für Schiefkörper mit Zentrum $\mathfrak{k}$ bzw. k gelten: *Die endlichen Schiefkörper $\mathfrak{S}/\mathfrak{k}$ einerseits und die endlichen unverzweigten Schiefkörper S/k mit Restklassenschiefkörper $\mathfrak{S}/\mathfrak{k}$ andererseits entsprechen sich gegenseitig. Im Sinne der Multiplikation der Algebrenklassen entsprechen sich dabei Produkte und Produkte.*

π sei ein festgewähltes Primelement von k. Dem zyklischen Körper $\mathfrak{Z}/\mathfrak{k}$ und einem seiner erzeugenden Automorphismen σ entspreche der unverzweigte zyklische Körper Z/k mit dem Automorphismus σ. Das *zyklische verschränkte Produkt* (π, Z, σ) ist dann ein verzweigter Schiefkörper über k. Es wird sich herausstellen, daß *alle verschränkten Produkte von dieser Gestalt im Sinne der Multiplikation der Algebrenklassen eine Gruppe ausmachen.*

Wir werden ferner feststellen, daß *jede Algebrenklasse* über k bei fester Wahl des Primelements π *eindeutig* durch *ein Produkt* $S \cdot (\pi, Z, \sigma)$ dargestellt werden kann. *Die Kenntnis aller Schiefkörper $\mathfrak{S}/\mathfrak{k}$ und aller zyklischen Körper $\mathfrak{Z}/\mathfrak{k}$ ermöglicht also eine Übersicht über alle Schiefkörper mit dem Zentrum k.* —

Für den Fall, daß $\mathfrak{k}$ die Charakteristik p hat, ist das Studium der Schiefkörper vom Exponenten p^n über k von besonderem Interesse. Da es wegen der Vollkommenheit von $\mathfrak{k}$ keine p-Schiefkörper $\mathfrak{S}/\mathfrak{k}$ gibt, kann dann jeder Schiefkörper vom Exponenten p^n über k in der Gestalt (π, Z, σ) dargestellt werden. Weil jeder zyklische Körper $\mathfrak{Z}/\mathfrak{k}$ vom Grad p^n durch eine Restklasse $a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \bmod p^n$ aus dem zu $\mathfrak{k}$ gehörigen p-adischen Körper charakterisiert werden kann, und zwar mit automatischer Festlegung eines erzeugenden Automorphismus σ, können wir diese Restklasse mod p^n als Invariante des Schiefkörpers (π, Z, σ) ansehen. Die Aufgabe, zu irgendeinem zyklischen verschränkten Produkt vom Grad p^n über k, auch mit verzweigtem zyklischen Körper, die so definierte zugehörige Invariante wirklich zu berechnen, ist schon gelöst worden für den Fall, daß k ebenfalls die Charakteristik p hat [1]). Wenn aber k die Charakteristik 0 hat, muß diese Aufgabe gleichfalls gelöst werden. Unter der Annahme, daß k eine primitive p^n-te Einheitswurzel ζ enthält, lautet also die *Aufgabe*:

[1]) E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p. Dieser Band, S. 126.

Explizite Bestimmung der Invariante der Algebra (a, b) *mit den Rechenregeln* $u^{p^n} = a$, $v^{p^n} = b$, $uvu^{-1}v^{-1} = \zeta$.

Die Lösung dieser Aufgabe enthält die explizite Formulierung des allgemeinen Reziprozitätsgesetzes für Zahlkörper.

1. $\bar{\mathfrak{k}}$ sei der algebraisch abgeschlossene Oberkörper von $\mathfrak{k}$, und $\bar{k}$ der unverzweigte Oberkörper von k mit $\bar{\mathfrak{k}}$ als Restklassenkörper.

Wir zeigen jetzt, daß es über $\bar{k}$ keine echten Schiefkörper gibt. Angenommen, $\bar{S}$ sei ein Schiefkörper über k. Da $\bar{S}/\bar{k}$ den Restklassengrad 1 hat, ist nach Hasse [2]) $\bar{S} = \bar{k}(\Pi)$ mit einem Primelement Π von $\bar{S}$. Also ist $\bar{S}$ kommutativ und kein echter Schiefkörper.

Aus dieser Tatsache ziehen wir jetzt den Schluß, daß eine normale Algebra A/k mindestens einen *unverzweigten* Zerfällungskörper K' hat. Da wir k als vollkommen angenommen haben, gibt es sogar einen unverzweigten *galoisschen* Zerfällungskörper K von A. Es sei $A \sim (a_{\sigma,\tau}, K)$.

Jedes Element a aus K läßt sich zerlegen in $\pi^e r \varepsilon$, wobei r dem multiplikativen Repräsentantensystem R von K entnommen ist, und wo $\varepsilon \equiv 1 \bmod \pi$ gilt. Entsprechend sei $a_{\sigma,\tau} = \pi^{e_{\sigma,\tau}} r_{\sigma,\tau} \varepsilon_{\sigma,\tau}$. Werden im Assoziativgesetz für $a_{\sigma,\tau}$ nur die Ordnungen $e_{\sigma,\tau}$ betrachtet, so folgt, daß auch $\pi^{e_{\sigma,\tau}}$ ein Faktorensystem ist, und daher auch $r_{\sigma,\tau}\varepsilon_{\sigma,\tau}$. Wird das Assoziativgesetz für $r_{\sigma,\tau}\varepsilon_{\sigma,\tau}$ nur mod π betrachtet, so folgt, weil die $r_{\sigma,\tau}$ dem multiplikativen Repräsentantensystem R angehören, daß $r_{\sigma,\tau}$ und damit auch $\varepsilon_{\sigma,\tau}$ ein Faktorensystem ist.

Für die willkürlich angenommene Algebra A/k *gilt* daher *eine Zerlegung*

$$A \sim (\pi^{e_{\sigma,\tau}}, K)\,(r_{\sigma,\tau}, K)\,(\varepsilon_{\sigma,\tau}, K) \qquad (r_{\sigma,\tau} \text{ aus } R,\ \varepsilon \equiv 1 \bmod \pi).$$

2. Zunächst behaupten wir, daß $(\varepsilon_{\sigma,\tau}, K)$ *zerfällt.*

Von $\varepsilon^{(1)}_{\sigma,\tau} = \varepsilon_{\sigma,\tau}$ ausgehend bilden wir auf folgende rekursive Weise die Faktorensysteme $\varepsilon^{(i)}_{\sigma,\tau} = 1 + \alpha^{(i)}_{\sigma,\tau}\pi^i$ mit ganzen $\alpha_{\sigma,\tau}$: Es sei $\varepsilon^{(i)}_{\sigma,\tau}$ schon konstruiert. Die $\alpha^{(i)}_{\sigma,\tau} \bmod \pi$ bilden dann ein Summandensystem im Restklassenkörper $\mathfrak{K}/\mathfrak{k}$. Wie ich in einer früheren Arbeit [3]) gezeigt habe, zerfällt ein solches Summandensystem stets, $\alpha^{(i)}_{\sigma,\tau} \equiv \beta^{(i)}_{\sigma} + \sigma\beta^{(i)}_{\tau} - \beta^{(i)}_{\sigma\tau} \bmod \pi$. Mit $\delta^{(i)}_{\sigma} = 1 - \beta^{(i)}_{\sigma}\pi^i$ bilden wir jetzt $\varepsilon^{(i+1)}_{\sigma,\tau} = \varepsilon^{(i)}_{\sigma,\tau}\delta^{(i)}_{\sigma}\delta^{(i)\sigma}_{\tau}\delta^{(i)-1}_{\sigma\tau}$. Es ist $\varepsilon^{(i+1)}_{\sigma,\tau} \equiv 1 \bmod \pi^{i+1}$. — Nach Bildung der Größen $\varepsilon^{(i)}_{\sigma,\tau}$ und $\delta^{(i)}_{\sigma}$ setzen wir $\prod_{i=1}^{\infty} \delta^{(i)}_{\sigma} = \delta_{\sigma}$. Es folgt $\varepsilon_{\sigma,\tau}\delta_{\tau}\delta^{\sigma}_{\tau}\delta^{-1}_{\sigma\tau} = 1$, also $(\varepsilon_{\sigma,\tau}, K) \sim 1$.

3. Nunmehr untersuchen wir die Algebra $U = (r_{\sigma,\tau}, K) = \sum_{\sigma} K u_{\sigma}$ mit den Regeln $u_{\sigma}u_{\tau} = r_{\sigma,\tau}u_{\sigma\tau}$ und $u_{\sigma}a u_{\sigma}^{-1} = a^{\sigma}$. Es sei K_0 die Maximalordnung von K. $U_0 = \sum_{\sigma} K_0 u_{\sigma}$ stellt dann eine Ordnung in U dar, und es ist

$$U_0/\pi U_0 \cong (\mathfrak{r}_{\sigma,\tau}, \mathfrak{K}) = \mathfrak{U},$$

wo $\mathfrak{r}_{\sigma,\tau}$ die Restklasse des Vertreters $r_{\sigma,\tau}$ darstellt. Die Diskriminante von $\mathfrak{U}$ verschwindet nicht, daher ist die Diskriminante der Ordnung $\mathfrak{U}_0 U_0$ nicht durch π teilbar, also Einheit. Also ist U_0 Maximalordnung, (π) ist darin Primideal, und U/k ist unverzweigt. Es sei $U = SM$ das Produkt eines Schiefkörpers S mit einem Matrizenring M. Nach Hasse [2]) gilt dann für die entsprechenden Maximalordnungen $U_0 \cong S_0 M_0$. Für die Restklassenringe folgt $\mathfrak{U} \sim \mathfrak{S}\mathfrak{M}$. Daraus ergibt sich:

---

[2]) H. Hasse, Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Math. Annalen **104** (1931).

[3]) E. Witt, Der Existenzsatz für abelsche Funktionenkörper, Crelle **173** (1935), S. 45 oben.

Der Restklassenring $\mathfrak{S}$ *des in der Algebra* $(r_{\sigma,\tau}, K)$ *steckenden Schiefkörpers* S *ist ein Schiefkörper mit dem Zentrum* $\mathfrak{k}$. S *ist unverzweigt.* S/k *und* $\mathfrak{S}/\mathfrak{k}$ *haben denselben Rang.*

Umgekehrt sei ein Schiefkörper $\mathfrak{S}/\mathfrak{k}$ vorgelegt. Es sei $\mathfrak{S} \cong (\mathfrak{r}_{\sigma,\tau}, \mathfrak{R})$ und $\mathfrak{R}/\mathfrak{k}$ trete als Restklassenkörper von K/k auf. Die zu K gehörigen multiplikativen Repräsentanten $r_{\sigma,\tau}$ der Restklassen $\mathfrak{r}_{\sigma,\tau}$ bilden wieder ein Faktorensystem. $\mathfrak{S}$ ist Restklassenring des in $(r_{\sigma,\tau}, K)$ steckenden Schiefkörpers S:

Jeder Schiefkörper $\mathfrak{S}/\mathfrak{k}$ *tritt als Restklassenring eines Schiefkörpers* S/k *auf.*

Wir beweisen weiter:

Der Schiefkörper S/k *ist durch seinen Restklassenring* $\mathfrak{S}/\mathfrak{k}$ *bis auf Isomorphie eindeutig bestimmt.*

Aus $S'S'' \sim S'''$ folgt $S'S'' = S'''M$. Für die Maximalordnungen folgt $S_0'S_0'' \cong S_0'''M_0$, und für die Restklassenringe $\mathfrak{S}'\mathfrak{S}'' \cong \mathfrak{S}'''\mathfrak{M}$ und damit $\mathfrak{S}'\mathfrak{S}'' \sim \mathfrak{S}'''$. Die Restklassenringzuordnung ist daher eine Homomorphie und wegen der Ranggleichheit sogar eine Isomorphie.

4. *Bei festem Primelement* π *bilden die Algebrenklassen* $(\pi^{e_{\sigma,\tau}}, K)$ *mit unverzweigten Körpern* K *eine Gruppe*:

Um das Produkt $(\pi^{e'_{\sigma,\tau}}, K')\,(\pi^{e''_{s,t}}, K'')$ zu bilden, werde $(\pi^{e'_{\sigma,\tau}}, K') \sim (\pi^{a_{S,T}}, K'K'')$ und $(\pi^{e''_{s,t}}, K'') \sim (\pi^{b_{S,T}}, K'K'')$ gesetzt. Das Produkt $(\pi^{a_{S,T}+b_{S,T}}, K'K'')$ hat dann die verlangte Gestalt.

Wir untersuchen jetzt eine feste Algebra $V = (\pi^{e_{\sigma,\tau}}, K)$ vom Grade g. Das Assoziativgesetz findet seinen Ausdruck in der Beziehung

$$e_{\sigma,\tau} + e_{\varrho,\sigma\tau} = e_{\varrho,\sigma} + e_{\varrho\sigma,\tau}$$

zwischen den ganzen Zahlen $e_{\sigma,\tau}$. Mit den rationalen Zahlen

$$\chi(\sigma) = \frac{1}{g}\sum_{\tau} e_{\sigma,\tau}$$

gilt, wie eine leichte Rechnung zeigt,

(a) $$e_{\sigma,\tau} = \chi(\sigma) + \chi(\tau) - \chi(\sigma\tau).$$

Der erlaubten Änderung der Zahlen $e_{\sigma,\tau}$ um Ausdrücke $d_\sigma + d_\tau - d_{\sigma\tau}$ mit ganzzahligen d_σ entspricht eine beliebige Abänderung der $\chi(\sigma)$ mod 1. Wir dürfen daher

(b) $$0 \leqq \chi(\sigma) < 1$$

annehmen.

Aus (a) folgt

$$\chi(\sigma) + \chi(\tau) \equiv \chi(\sigma\tau) \bmod 1,$$

d. h. $\chi(\sigma)$ ist mod 1 ein Charakter der Gruppe $\mathfrak{G}$ von K/k. Es sei dabei $\mathfrak{N}$ der durch $\chi(\nu) \equiv 0 \bmod 1$ bestimmte Normalteiler von $\mathfrak{G}$. $\mathfrak{G}/\mathfrak{N}$ ist der zyklischen Wertegruppe von $\chi(\sigma)$ mod 1 isomorph. Aus $\sigma \equiv s$, $\tau \equiv t \bmod \mathfrak{N}$ folgt wegen der Normierung (b) $\chi(\sigma) = \chi(s)$ und somit nach (a) $e_{\sigma,\tau} = e_{s,t}$. Es ist daher $V \sim (\pi^{e_{\sigma,\tau}}, Z)$, wobei Z/k den nach der Galoisschen Theorie zu $\mathfrak{G}/\mathfrak{N}$ gehörigen zyklischen Körper vom Grad n bedeutet. Wird jetzt speziell mit s derjenige Automorphismus von Z/k mit $\chi(s) = \frac{1}{n}$ bezeichnet, so erzeugt s die Gruppe von Z/k, und es ist

$$(\pi^{e_{\sigma,\tau}}, K) \sim (\pi, Z, s).$$

Da π^n die niedrigste Potenz von π ist, die Norm einer Zahl aus dem unverzweigten zyklischen Körper Z/k n-ten Grades sein kann, hat (π, Z, s) den Exponenten n und ist

folglich ein Schiefkörper. Nach Hasse [2]) hat der Schiefkörper $(\pi, Z, s) = \sum_0^{n-1} Z u^i$ mit den Regeln $u^n = \pi$ und $uau^{-1} = a^s$ die Maximalordnung $\sum_0^{n-1} Z_0 u^i$. In dieser Maximalordnung ist (u) Primideal, also ist der Schiefkörper verzweigt von der Ordnung n. $\mathfrak{Z}$ ist der Restklassenring mod u.

5. Damit haben wir nachgewiesen:

Für jede Algebra A/k besteht eine Zerlegung

$$A \sim S \cdot (\pi, Z, \sigma);$$

dabei ist S als unverzweigter Schiefkörper durch seinen Restklassenschiefkörper $\mathfrak{S}$ festgelegt, und der unverzweigte zyklische Körper Z mit dem Automorphismus σ durch den Restklassenkörper $\mathfrak{Z}$ mit dem Automorphismus σ.

Es folgt nun leicht:

Nach angenommener Wahl des Primelements π ist die Zerlegung von A eindeutig.

Denn der erste Faktor gehört der Gruppe der unverzweigten Schiefkörper an, und der zweite Faktor gehört zu einer Gruppe aus lauter verzweigten Schiefkörpern, die beiden Gruppen sind also fremd.

Eingegangen 29. August 1936.

Zerfallende zyklische p-Algebren.

Von *Oswald Teichmüller* in Göttingen.

Diese Arbeit schließt sich unmittelbar an eine vorangehende von E. Witt[1]) an. Erst wird hier der Haupthilfssatz für den Beweis der Residuenformel (Satz 17 jener Arbeit) bewiesen, dann ergibt sich aus dem Beweis ein Kriterium für den Zerfall von Algebren $(\alpha\,|\,\beta]$.

Es handelt sich um folgenden

Hilfssatz. *Ist $k = C\{t\}$ der Potenzreihenkörper über dem vollkommenen Grundkörper C und enthalten die Potenzreihen $\beta_0, \ldots, \beta_{n-1}$ nur die Glieder mit negativen Potenzen von t:*

$$\beta_\nu = \sum_{i=-w_\nu}^{-1} b_{\nu i} t^i ,$$

so gilt über k

$$(t\,|\,\beta] \sim 1 .$$

Statt dessen beweisen wir gleich den etwas allgemeineren

Satz 1. *C sei ein vollkommener Unterkörper eines Körpers k der Charakteristik p. Für $\alpha \neq 0$ aus k bilden wir den Ring*

$$R = C\alpha + C\alpha^2 + \cdots .$$

Für $\beta_0, \ldots, \beta_{n-1}$ in R gilt dann

$$(\mathfrak{A}) \qquad (\alpha\,|\,\beta_0, \ldots, \beta_{n-1}] \sim 1 .$$

Dieser Satz enthält offenbar den obigen Hilfssatz, man nehme $\alpha = t^{-1}$.

Satz 1 gelte schon für $n-1$, wir beweisen ihn für n. Nach W. Satz 15 besagt unsere Induktionsvoraussetzung genau, daß $(\mathfrak{A})$ jedenfalls für $\beta_0 = 0$ gilt. Man beachte, daß so auch der Fall $n = 1$ mitgenommen wird.

Wir bemerken noch vorweg, daß für zwei Vektoren x und y aus R auch $x \pm y$ und $\wp x$ Komponenten aus R haben. Denn R ist ein Ring; daß R kein Einselement zu haben braucht, spielt keine Rolle.

Um nun $(\mathfrak{A})$ zu beweisen, zeigen wir zunächst

$$(\alpha\,|\,\alpha, 0, \ldots, 0] \sim 1 ;$$

hieraus wird sich später leicht die allgemeine Formel ergeben. Außerdem machen wir noch eine Fallunterscheidung, je nachdem $\alpha = \wp a$, $a \in k$, ist oder nicht.

Ist $\alpha = \wp a$, so sei entsprechend W. (20)

$$(\alpha, 0, \ldots, 0) = \wp(a, 0, \ldots, 0) + (0, \eta_1, \ldots, \eta_{n-1}),$$

---

[1]) E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, dieser Band, S. 126, zitiert mit W.

dann sind die $\eta_1, \ldots, \eta_{n-1}$ in

$$R' = Ca + Ca^2 + \cdots,$$

und nach W. (22) und der Induktionsvoraussetzung haben wir

$$(a\,|\,\alpha, 0, \ldots, 0] \cong (a\,|\,0, \eta_1, \ldots, \eta_{n-1}] \sim 1.$$

Weil für alle i des Primkörpers auch $\wp(a+i) = \alpha$ ist, gilt genau so

$$(a+i\,|\,\alpha, 0, \ldots, 0] \sim 1;$$

durch Multiplikation folgt

$$(\alpha\,|\,\alpha, 0, \ldots, 0] \sim 1,$$

weil doch $\prod_{i=0}^{p-1}(a+i) = \wp a = \alpha$ ist.

Wenn aber $\alpha \neq \wp a$ ist, so ist nach W. Satz 13

$$Z_n = k(\Theta_0, \ldots, \Theta_{n-1}) \quad \text{mit} \quad \wp\Theta = (\alpha, 0, \ldots, 0)$$

ein zyklischer Körper mit dem erzeugenden Automorphismus

$$\sigma\Theta = \Theta + 1.$$

Wir betrachten den Zwischenkörper

$$Z_1 = k(\Theta_0)$$

und in ihm den Ring

$$R' = C\Theta_0 + C\Theta_0^2 + \cdots.$$

Wieder sei

$$(\mathfrak{B}) \qquad (\alpha, 0, \ldots, 0) = \wp(\Theta_0, 0, \ldots, 0) + (0, \mathsf{H}_1, \ldots, \mathsf{H}_{n-1}),$$

die $\mathsf{H}_1, \ldots, \mathsf{H}_{n-1}$ liegen dann in R'. Nach Induktionsvoraussetzung gilt

$$(\mathfrak{C}) \qquad (\Theta_0\,|\,\mathsf{H}_1, \ldots, \mathsf{H}_{n-1}] \sim 1.$$

Aus $(\mathfrak{B})$ folgt aber auch

$$Z_n = Z_1\left(\frac{(\alpha, 0, \ldots, 0)}{\wp}\right) = Z_1\left(\frac{(\mathsf{H}_1, \ldots, \mathsf{H}_{n-1})}{\wp}\right),$$

d. h. Z_n ist der kleinste Zerfällungskörper des Vektors $(\mathsf{H}_1, \ldots, \mathsf{H}_{n-1})$ aus Z_1. Indem man gemäß der Bemerkung nach W. Satz 15 die Algebra $(\Theta_0\,|\,\mathsf{H}_1, \ldots, \mathsf{H}_{n-1}]$ als zyklische Algebra auffaßt, sieht man aus $(\mathfrak{C})$, daß $\Theta_0 = N_{Z_n/Z_1}\Xi$ Norm eines Elements von Z_n ist. Offenbar ist aber $\alpha = N_{Z_1/Z_0}\Theta_0$, mithin

$$\alpha = N_{Z_n/Z_0}\Xi.$$

Deshalb muß die zyklische Algebra $(\alpha\,|\,\alpha, 0, \ldots, 0]$ zerfallen.

Um nun $(\mathfrak{A})$ zu beweisen, bemerken wir zuerst, daß $(\alpha\,|\,\beta_0, \ldots, \beta_{n-1}]$ für $\beta_\nu \in R$ nach Induktionsvoraussetzung nur von β_0 abhängt und daß aus $\beta_0 + \beta_0' = \bar{\beta}_0$ folgt

$$(\alpha\,|\,\beta_0, \ldots, \beta_{n-1}] \times (\alpha\,|\,\beta_0', \ldots, \beta_{n-1}'] \sim (\alpha\,|\,\bar{\beta}_0, \ldots, \bar{\beta}_{n-1}].$$

Es genügt darum,

$$(\mathfrak{D}) \qquad (\alpha\,|\,c\alpha^r, 0, \ldots, 0] \sim 1 \qquad (c \in C,\ r > 0)$$

zu beweisen. $c = 0$ wäre trivial, es sei $c \neq 0$.

Ist r zu p prim, so ist

$$(\mathfrak{E}) \qquad (\alpha\,|\,c\alpha^r, 0, \ldots, 0]^r \times \left(\sqrt[p^n]{c}\,|\,c\alpha^r, \ldots, 0\right]^{p^n} \sim (c\alpha^r\,|\,c\alpha^r, 0, \ldots, 0] \sim 1;$$

weil die p^n-te Potenz jeder unserer Algebren ~ 1 ist, ergibt sich daraus $(\mathfrak{D})$.

Ist aber $r = ps$, so kann ($\mathfrak{D}$) für s statt r schon als richtig angesehen werden, und ($\mathfrak{D}$) folgt dann aus

$$(c\alpha^{ps}, 0, 0, \ldots, 0) = \left(\sqrt[p]{c}\,\alpha^s, 0, \ldots, 0\right) + \wp\left(\sqrt[p]{c}\,\alpha^s, 0, \ldots, 0\right) + (0, \delta_1, \ldots, \delta_{n-1}), \quad \delta_\nu \in R.$$

Damit ist Satz 1 bewiesen. Nun soll für jedes feste $\alpha \neq 0$ aus einem beliebigen Körper k der Charakteristik p die additive Gruppe aller Vektoren β mit $(\alpha|\beta_0, \ldots, \beta_{n-1}] \sim 1$ bestimmt werden.

Natürlich ist $(\alpha|\wp\gamma] \sim 1$. Ferner gilt nach dem soeben bewiesenen Satze $(\alpha|\alpha, 0, \ldots, 0] \sim 1$. (Für das oben auftretende C kann man z. B. den Primkörper nehmen.) Wie bei ($\mathfrak{E}$) folgt daraus für $(r, p) = 1$

$$(\alpha|c^{p^n}\alpha^r, 0, \ldots, 0]^r\,(c|c^{p^n}\alpha^r, 0, \ldots, 0]^{p^n} \sim (c^{p^n}\alpha^r|c^{p^n}\alpha^r, 0, \ldots, 0] \sim 1,$$
$$(\alpha|c^{p^n}\alpha^r, 0, \ldots, 0] \sim 1.$$

Wir behaupten nun, daß damit schon im wesentlichen die gesuchte additive Gruppe aufgefunden ist:

Satz 2. *Ist* $(\alpha|\beta] \sim 1$, *so ist* β *von der Form*

$$(\mathfrak{F}) \quad \beta = \wp\gamma + \sum_{r=1}^{p-1} V^{n-1}(c_{n-1,r}^{p}\alpha^r) + \sum_{\substack{r=1\\ p\nmid r}}^{p^2-1} V^{n-2}(c_{n-2,r}^{p^2}\alpha^r, 0) + \cdots + \sum_{\substack{r=1\\ p\nmid r}}^{p^n-1} (c_{0,r}^{p^n}\alpha^r, 0, \ldots, 0).$$

Ist dieser Satz schon für Vektoren mit $n-1$ Komponenten richtig, so genügt es offenbar, aus $(\alpha|\beta] \sim 1$ eine Darstellung

$$\beta_0 = \wp c_0 + \sum_{\substack{r=1\\ p\nmid r}}^{p^n-1} c_r^{p^n}\alpha^r$$

zu folgern, dann wird nämlich durch

$$(\beta_0, \ldots, \beta_{n-1}) = \wp(c_0, 0, \ldots, 0) + \sum_{\substack{r=1\\ p\nmid r}}^{p^n-1} (c_r^{p^n}\alpha^r, 0, \ldots, 0) + (0, \beta_1', \ldots, \beta_{n-1}')$$

ein Vektor $(\beta_1', \ldots, \beta_{n-1}')$ mit $n-1$ Komponenten definiert, für den auch $(\alpha|\beta'] \sim 1$ gilt und der darum schon die Struktur ($\mathfrak{F}$) haben muß.

Wenn α in k eine p-te Potenz sein sollte: $\alpha = \delta^p$, so gilt

$$(\alpha|\beta] \sim (\delta|\beta]^p \sim (\delta|p\beta] \sim (\delta|V\beta^p] \sim (\delta|V\beta^p - \wp V\beta] \sim (\delta|V\beta];$$

aus $(\alpha|\beta_0, \ldots, \beta_{n-1}] \sim 1$ folgt also $(\delta|\beta_0, \ldots, \beta_{n-2}] \sim 1$; weil hier nur eine Algebra vom Grad p^{n-1} auftritt, gilt schon eine Darstellung

$$\beta_0 = \wp c' + \sum_{\substack{r=1\\ p\nmid r}}^{p^{n-1}-1} c_r^{p^{n-1}}\delta^r,$$

aus ihr folgt

$$\beta_0 = \beta_0^p - \wp\beta_0 = \wp(c'^p - \beta_0) + \sum_{\substack{r=1\\ p\nmid r}}^{p^{n-1}-1} c_r^{p^n}\alpha^r.$$

Dies gilt für $n > 1$; ist $n = 1$ und $\alpha = \delta^p$, so ist einfach

$$\beta_0 = \wp(-\beta_0) + \left(\frac{\beta_0}{\delta}\right)^p \alpha.$$

Nun sei α keine p-te Potenz. Wir betrachten die beiden Algebren

$$A = (\alpha|\beta] = k[u, \Theta_\nu], \quad u^{p^n} = \alpha, \quad \wp\Theta = \beta, \quad u\Theta u^{-1} = \Theta + 1$$

und

$$A^{(0)} = (\alpha\,|\,0] = k[u, \Theta_\nu^{(0)}], \quad u^{p^n} = \alpha, \quad \wp\Theta^{(0)} = 0, \quad u\Theta^{(0)}u^{-1} = \Theta^{(0)} + \mathbf{1}.$$

Sie sollen ähnlich sein, also müssen sie durch einen Isomorphismus i. b. a. k ineinander übergehen; dieser Isomorphismus kann sogar so gewählt werden, daß die kommutativen Unterkörper $k(u)$ von $A^{(0)}$ und von A einander entsprechen. Wir denken uns also A und $A^{(0)}$ als dieselbe Algebra mit demselben u darin.

Aus $u\Theta_0 u^{-1} = \Theta_0 + 1$ und $u\Theta_0^{(0)}u^{-1} = \Theta_0^{(0)} + 1$ folgt

$$\Theta_0 - \Theta_0^{(0)} = y \in k(u),$$

denn y ist mit u vertauschbar und $k(u)$ ist maximalkommutativ. Es sei

$$y = \sum_{r=0}^{p^n-1} c_r u^r = \sum_{s=0}^{p-1} \left(\sum_{h=0}^{p^{n-1}-1} c_{hp+s} (u^p)^h \right) u^s, \quad c_r \in k.$$

Betrachten wir nun die Subalgebra $k[u, \Theta_0^{(0)}]$ als einfache und normale Algebra über ihrem Zentrum $k(u^p)$, so ist nach einem früheren Ergebnis von Witt [2])

$$(\mathfrak{G}) \qquad \beta_0 = \wp(\Theta_0^{(0)} + y) = \wp\Theta_0^{(0)} + \mathfrak{p}_u y = \sum_{r=0}^{p^n-1} c_r^p u^{pr} - \sum_{h=0}^{p^{n-1}-1} c_{hp} u^{hp}.$$

Um den rechtsstehenden Ausdruck auszuwerten, zerspalten wir y folgendermaßen:

$$y = \sum_{\nu=0}^{n} s_\nu; \qquad s_\nu = \sum_{\substack{t=1 \\ p \nmid t}}^{p^{n-\nu}-1} c_{tp^\nu} u^{tp^\nu} \quad (\nu = 0, \ldots, n-1), \qquad s_n = c_0.$$

Wir fassen also die $c_r u^r$ nach der in r steckenden p-Potenz zusammen. Dann geht $(\mathfrak{G})$ über in

$$(\mathfrak{H}) \qquad \beta_0 = (s_0 + \cdots + s_{n-1} + s_n)^p - s_1 - \cdots - s_n = (s_0^p - s_1) + (s_1^p - s_2) + \cdots + (s_{n-2}^p - s_{n-1}) + (s_{n-1}^p + s_n^p - s_n).$$

β_0 liegt aber in k. Wir sehen also, daß man y nicht ganz beliebig vorschreiben darf, sondern daß wir darauf achten müssen, daß bei Entwicklung der rechten Seite von $(\mathfrak{H})$ nach Potenzen von u ein Element von k erscheint. $s_{n-1}^p + s_n^p - s_n = \wp c_0 + s_{n-1}^p$ liegt schon in k, aber die übrigen Glieder $s_\nu^p - s_{\nu+1}$ $(\nu = 0, 1, \ldots, n-2)$ enthalten u-Potenzen mit genau durch $p^{\nu+1}$ teilbarem Exponenten, sie müssen also alle verschwinden. Das heißt

$$s_0^p = s_1, \quad s_1^p = s_2, \ldots, \quad s_{n-2}^p = s_{n-1},$$
$$\beta_0 = \wp c_0 + s_{n-1}^p$$

oder

$$\beta_0 = \wp c_0 + s_0^{p^n} = \wp c_0 + \sum_{\substack{t=1 \\ p \nmid t}}^{p^n-1} c_t^{p^n} \alpha^t, \qquad \text{w. z. b. w.}$$

Wir haben damit T. Satz 8 auf zyklische p-Algebren vom Grad p^n übertragen. Dagegen macht die Übertragung des (mehr besagenden) Satzes 7 noch Schwierigkeiten. Ich hoffe, sie durch eine Verallgemeinerung meiner Normierung [3]) für p^2 auf p^n beheben zu können.

---

[2]) Veröffentlicht in: O. Teichmüller, p-Algebren, Deutsche Mathematik **1** (1936), Satz 7. Zitiert mit T.

[3]) O. Teichmüller, Multiplikation zyklischer Normalringe, Deutsche Mathematik **1** (1936), § 15: Zyklische Normalringe vom Rang p^2.

Eingegangen 29. August 1936

Zur Arithmetik der zyklischen p-Körper.

Von *Hermann Ludwig Schmid* in Göttingen.

Unter einem zyklischen p-Körper Z/K verstehe ich einen zyklischen Erweiterungskörper Z vom Grade p^n $(n \geqq 1)$ über einem algebraischen Funktionenkörper K mit einem vollkommenen Konstantenkörper k der Charakteristik p. In einer früheren Arbeit habe ich gezeigt, wie man zu einer brauchbaren normierten Erzeugung von Z über K gelangen kann [1]). Im Anschluß an meine Arbeit hat Herr Witt einen Vektorkalkül entwickelt, der die geeignete Schreibweise für meine Resultate liefert [2]). Darüber hinaus gelang Herrn Witt die Verallgemeinerung der von mir für den Grad p aufgestellten Residuenformel.

Ich wiederhole hier kurz die von mir aufgestellten arithmetischen Sätze in der neuen Schreibweise. Anschließend entwickle ich die Theorie des Führers, der Diskriminante und des Geschlechts. Schließlich beantworte ich die Frage, ob die Verzweigungspunkte Weierstraßpunkte sind.

Die Arithmetik der zyklischen p-Körper ist in der jetzigen Form eine fast wörtliche Verallgemeinerung der von Herrn Hasse für den Fall des Grades p gewonnenen arithmetischen Sätze [3]). Man hat nur Elemente durch Vektoren und die gewöhnliche Addition durch die Wittsche Vektoraddition zu ersetzen.

1. k sei ein vollkommener Körper der Charakteristik p $(p > 0)$ und K ein algebraischer Funktionenkörper einer Unbestimmten mit k als Konstantenkörper. $\beta = (\beta_1, \ldots, \beta_n)$ sei ein n-gliedriger Vektor mit Komponenten β_i aus K. Es sei $\beta_1 \neq \wp\gamma$ mit γ aus K. Dann wird durch den Vektor $\theta = (\theta_1, \ldots, \theta_n)$, der der Vektorgleichung (im Wittschen Sinne)

$$\dot{\wp}\theta = \theta^p \dot{-} \theta = \beta$$

genügt [4]), ein zyklischer Körperturm

$$Z_1 = K(\theta_1), \quad Z_2 = Z_1(\theta_2), \ldots, Z_n = Z_{n-1}(\theta_{n-1})$$

---

[1]) H. L. Schmid, Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p, Crelles Journal **175** (1936). Im folgenden zitiert mit S.

[2]) E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grade p^n. Struktur diskret bewerteter Körper mit vollkommenem Restklassenkörper der Charakteristik p, Crelles Journal **176** (1936).

[3]) H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, Crelles Journ. **172** (1934).

[4]) Ich schreibe, um jedes Mißverständnis auszuschließen, für die neue Vektoraddition das Symbol $\dot{+}$. Die Vektorgleichung $\dot{\wp}\theta = \beta$ ist gleichwertig mit dem System von Gleichungen $\wp\theta_\nu = \beta_\nu + z_{\nu-1}$ $(z_0 = 0;\ \nu = 1, \ldots, n)$, wo die z_ν formal für Charakteristik 0 durch

$$z_\nu = \sum_{i=1}^{\nu} \frac{1}{p^{\nu-i+1}} \left[\theta_i^{p^{\nu-i+1}} + \beta_i^{p^{\nu-i+1}} - (\theta_i + \beta_i + z_{i-1})^{p^{\nu-i+1}}\right]$$

rekursiv erklärt sind.

vom Grade p^n erzeugt. Ein erzeugender Automorphismus σ wird durch

$$\sigma = (\theta \to \theta \dot{+} e)$$

gegeben, wo e den Vektor $(1, 0, \ldots, 0)$ bedeutet.

Die Wittsche Vektoraddition ist so gewählt, daß sie gerade diejenige normierte Erzeugung liefert, die in S die Rolle eines Existenznachweises spielt. Man kann natürlich für jede in S zugelassene Normierung einen analogen Kalkül aufbauen, der in derselben Weise zur Erzeugung der zyklischen p-Körper geeignet ist.

2. Für jede Stelle $\mathfrak{p}$ von K seien die Komponenten des Vektors β durch zulässige Substitutionen $\theta \to \theta \dot{+} \gamma$ mit einem Vektor γ aus K auf die Form

$$\beta_i \cong \frac{\mathfrak{g}_i}{\mathfrak{p}^{\lambda_i}} \left(\lambda_i \geqq 0; \begin{array}{l}(\lambda_i, p) = 1 \text{ und } \mathfrak{g}_i \text{ prim zu } \mathfrak{g}, \text{ falls } \lambda_i > 0; \\ \mathfrak{g}_i \text{ ganz für } \mathfrak{p}, \text{ falls } \lambda_i = 0; \quad i = 1, \ldots, n\end{array}\right)$$

gebracht [5]). Der Zahlenvektor $\lambda = (\lambda_1, \ldots, \lambda_n)$ gibt dann über Zerlegung bzw. Verzweigung Auskunft:

Der Primdivisor $\mathfrak{p}$ bleibt dann und nur dann in Z_n unverzweigt, wenn λ der Nullvektor ist. Tritt beim Übergang von $Z_{\mu-1}$ nach Z_μ $(1 \leqq \mu < n)$ zum ersten Male Trägheit ein, so gilt dies auch für alle folgenden Schritte, soweit sie überhaupt unverzweigt sind.

Ist insbesondere k ein Galoisfeld von $q = p^f$ Elementen, so können wir im unverzweigten Falle den *Artin-Automorphismus*

$$F = \left(\theta \to \theta \dot{+} \left\{\frac{\beta}{\mathfrak{p}}\right\}\right) \quad \text{mit } z^F \equiv z^{\mathfrak{N}\mathfrak{p}} \bmod \mathfrak{p}$$

für alle für $\mathfrak{p}$ ganzen z einführen. Es ist

$$\left\{\frac{\beta}{\mathfrak{p}}\right\} \equiv \dot{\mathfrak{S}}(\dot{S}_{\mathfrak{p}}(\beta)) \bmod \mathfrak{p},$$

wo der Vektor $\dot{S}_{\mathfrak{p}}(\beta) \equiv \beta + \beta^q \dot{+} \cdots \dot{+} \beta^{\overline{\frac{\mathfrak{N}\mathfrak{p}}{q}}} \bmod \mathfrak{p}$ die *punktierte Spur* im Sinne der Vektoraddition im Restklassenkörper mod $\mathfrak{p}$ von K in bezug auf den Konstantenkörper k und $\dot{\mathfrak{S}}$ entsprechend die *absolute punktierte Spur* von k (in bezug auf den Primkörper) bezeichnet.

Denn wird die F definierende Kongruenz auf den erzeugenden Vektor θ angewandt, so ergibt sich

$$\theta^{\mathfrak{N}\mathfrak{p}} = \theta \dot{+} \beta + \beta^p + \cdots \dot{+} \beta^{\overline{\frac{\mathfrak{N}\mathfrak{p}}{p}}} \equiv \dot{\mathfrak{S}}(\dot{S}_{\mathfrak{p}}(\beta)) \bmod \mathfrak{p}.$$

$\mathfrak{p}$ zerfällt hiernach in Z_n dann und nur dann voll, wenn die Kongruenzen $\beta \equiv \dot{\wp}\beta^{(0)} \bmod \mathfrak{p}$ mit einem Vektor $\beta^{(0)} = (\beta_1^{(0)}, \ldots, \beta_n^{(0)})$ aus K lösbar sind. Allgemeiner ist der Grad von $\mathfrak{p}$ in Z_n gleich der Ordnung des Vektors β in bezug auf die Gruppe der $\dot{\wp}\beta^{(0)} \bmod \mathfrak{p}$. Für das Symbol $\left\{\frac{\beta}{\mathfrak{p}}\right\}$ gilt die Regel

$$\left\{\frac{\beta \dot{+} \beta'}{\mathfrak{p}}\right\} = \left\{\frac{\beta}{\mathfrak{p}}\right\} \dot{+} \left\{\frac{\beta'}{\mathfrak{p}}\right\}$$

für zwei Vektoren β und β'. Das *zusammengesetzte Artin-Symbol* definieren wir durch den Vektor

$$\left\{\frac{\beta}{\mathfrak{a}}\right\} = \dot{\sum_{\mathfrak{p}}} \left\{\frac{\beta}{\mathfrak{p}}\right\},$$

---

[5]) Die Möglichkeit dieser Reduktion ist für den Fall des Grades p in der zitierten Arbeit von Herrn Hasse gezeigt. Allgemein ergibt sich die Reduktionsmöglichkeit durch Induktion nach n.

wenn $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}$ (gleiche $\mathfrak{p}$ zugelassen) ein ganzer Divisor ist, dessen Primteiler in Z_n sämtlich unverzweigt sind. Für dieses Symbol gilt das Reziprozitätsgesetz, dessen Kernaussage lautet: Es ist

$$\left\{\frac{\beta}{\mathfrak{a}}\right\} = (0, \ldots, 0), \quad \text{wenn} \quad \mathfrak{a} \sim N\mathfrak{A} \bmod \mathfrak{f},$$

wo $\mathfrak{A}$ ein zum Führer $\mathfrak{f}$ von Z_n primer Divisor aus Z_n ist.

3. *$\mathfrak{p}$ ist dann und nur dann in Z_n verzweigt, wenn λ verschieden vom Nullvektor ist. Ist λ_μ die erste von Null verschiedene Komponente, so tritt von $Z_{\mu-1}$ ab Vollverzweigung ein.*

Es sei jetzt o. B. d. A. bereits $\lambda_1 > 0$. Dann ist $\mathfrak{p}$ in Z_n vollverzweigt. Es sei $\mathfrak{p} = \mathfrak{P}_1^p = \mathfrak{P}_2^{p^2} = \cdots = \mathfrak{P}_n^{p^n}$, wo $\mathfrak{P}_i$ den Primteiler von $\mathfrak{p}$ in Z_i bezeichnen möge. Wir beweisen den

Satz. *Der $\mathfrak{p}$-Beitrag zum Führer von Z_n über K ist $\mathfrak{f}_{\mathfrak{p}}^{(n)} = \mathfrak{p}^{M_n+1}$ mit $M_n = \operatorname{Max}_{i=1,\ldots,n} (p^{n-i}\lambda_i)$.*

Wir bemerken vorweg, daß wegen $M_i = \operatorname{Max}(pM_{i-1}, \lambda_i)$ die Zahlen M_i eine aufsteigende Folge bilden: $M_1 < M_2 < \cdots < M_n$. Weiterhin kann das Maximum M_n nur von einem Wert $p^{n-i}\lambda_i$ erreicht werden, weil aus $p^{n-i}\lambda_i = p^{n-j}\lambda_j$ mit $j > i$ die Gleichheit $p^{j-i}\lambda_i = \lambda_j$ folgen würde in Widerspruch zu $(\lambda_j, p) = 1$. Es sei

$$M_n = p^{n-j}\lambda_j \qquad (1 \leqq j \leqq n).$$

Den Beweis der Führerformel erbringen wir mit Hilfe der Wittschen Residuenformel

$$(\alpha; \beta] \sim (\pi; (\alpha, \beta)].$$

Dabei ist π ein Primelement zu $\mathfrak{p}$ und (α, β) der sogenannte Residuenvektor zur Algebra $(\alpha; \beta]$, die durch die erzeugenden Relationen $u^{p^n} = \alpha$, $\varphi\theta = \beta$, $u\theta u^{-1} = \theta + e$ definiert ist. Wir zeigen dann

a) Wenn $\alpha \equiv 1 \bmod \pi^{M_n+1}$ ist, ist α Norm eines Elementes aus $Z_n\mathfrak{P}_n$ in bezug auf $K_{\mathfrak{p}}$.

b) Es existiert ein $\alpha \equiv 1 \bmod \pi^{M_n}$ so, daß α nicht Norm ist.

Bei der Ausrechnung des Residuenvektors müssen α und die Komponenten von β als Potenzreihenunbestimmte angesetzt und es muß formal in einem Körper der Charakteristik Null gerechnet werden. Wir wollen aber keine neuen Bezeichnungen einführen und uns die Abstraktion bei der Rechnung vor Augen halten. Es sei

$$\alpha = 1 + c\pi^{M_n} + \cdots$$

und

$$\beta_i = \frac{b_i}{\pi^{\lambda_i}} + \cdots \qquad (i = 1, \ldots, n).$$

Ausgehend von den Nebenkomponenten

$$\beta^{(\nu)} = \sum_{i=1}^{\nu} p^{i-1} \beta_i^{p^{\nu-i}}$$

des Vektors

$$\beta = (\beta_1, \ldots, \beta_n)$$

werden die Nebenkomponenten des Residuenvektors (α, β) erklärt durch

$$(\alpha, \beta)^{(\nu)} = \operatorname{Res} \frac{d\alpha}{\alpha} \beta^{(\nu)}.$$

Es ist

$$\frac{d\alpha}{\alpha} \beta^{(\nu)} = \left(cM_n\pi^{M_n} \frac{d\pi}{\pi} + \cdots\right)\left(\sum_{i=1}^{\nu} p^{i-1} \frac{b_i^{p^{\nu-i}}}{\pi^{\lambda_i p^{\nu-i}}} + \cdots\right).$$

Das Residuum hiervon ist

$$(\alpha, \beta)^{(\nu)} = 0 \quad \text{für } \nu < n,$$
$$(\alpha, \beta)^{(n)} = c\, p^{n-1} \lambda_j b_j^{p^{n-j}}.$$

Durch Übergang zu den Hauptkomponenten folgt jetzt

$$(\alpha, \beta) = (0, \ldots, 0, b_j^{p^{n-j}} c\lambda_j).$$

Die Residuenformel ergibt nun

$$(\alpha; \beta] \sim (\pi; 0, \ldots, 0, b_j^{p^{n-j}} c\lambda_j] \sim (\pi; b_j^{p^{n-j}} c\lambda_j].$$

Einerseits ist also $(\alpha; \beta] \sim 1$ für $c = 0$; andererseits kann man aber c so bestimmen, daß die Algebra $(\pi; b_j^{p^{n-j}} c\lambda_j]$ nicht zerfällt. Dadurch ist unsere Behauptung bewiesen.

Differente $\mathfrak{D}^{(n)}$ und *Diskriminante* $\mathfrak{d}^{(n)}$ von Z_n über K berechnen wir mit Hilfe der Führer-Diskriminantenformel [6])

$$\mathfrak{d}_\mathfrak{p} = \prod_\chi \mathfrak{f}_\mathfrak{p}(\chi).$$

Dabei durchläuft χ alle Charaktere der zyklischen Gruppe $\mathfrak{Z}_n$ von Z_n/K und $\mathfrak{f}_\mathfrak{p}(\chi)$ bedeutet den $\mathfrak{p}$-Führer desjenigen Teilkörpers von Z_n/K, der zu der durch $\chi = 1$ charakterisierten Untergruppe von $\mathfrak{Z}_n$ gehört. Dies ergibt in unserem Falle:

$$\mathfrak{d}_\mathfrak{p}^{(n)} = \prod_{i=1}^{n} \mathfrak{f}_\mathfrak{p}^{(i)\,\varphi(p^i)} = \prod_{i=1}^{n} \mathfrak{f}_\mathfrak{p}^{(i)\,p^i - p^{i-1}} \qquad (\varphi \text{ Eulersche Funktion}).$$

Also wird der $\mathfrak{p}$-Beitrag zur Diskriminante $\mathfrak{d}^{(n)}$

$$\mathfrak{d}_p^{(n)} = \mathfrak{p}^D \quad \text{mit} \quad D = \sum_{i=1}^{n} (p^i - p^{i-1})(M_i + 1)$$

und der $\mathfrak{p}$-Beitrag zur Differente $\mathfrak{D}^{(n)}$

$$\mathfrak{D}_{\mathfrak{P}_n}^{(n)} = \mathfrak{P}_n^D.$$

Die Komponenten des Zahlenvektors $\lambda = (\lambda_1, \ldots, \lambda_n)$ sind keiner Größenbeziehung untereinander unterworfen. Wir beweisen nun den interessanten

Satz. *Wird Z_n über Z_1 durch den Vektor $(\beta_2', \ldots, \beta_n')$ erzeugt, so sind die Komponenten des entsprechend gebildeten (d. h. für $\mathfrak{P}_1$ reduzierten) Vektors $\lambda' = (\lambda_2', \ldots, \lambda_n')$ der Größe nach angeordnet. Es gilt $\lambda_i' = pM_i - (p-1)M_1$ $(i = 2, \ldots, n)$.*

Wir bemerken nebenbei, daß sich die Komponenten $(\beta_2', \ldots, \beta_n')$ leicht angeben lassen. Sie sind offenbar die 2. bis n-ten Komponenten des Vektors $\beta \dotplus \bar{\theta}$ mit $\bar{\theta} = (\theta_1, 0, \ldots, 0)$.

Beweis. Führer bzw. Diskriminante und Differente von Z_ν über Z_1 $(\nu = 1, \ldots, n)$ seien mit $\mathfrak{f}'^{(\nu)}$ bzw. $\mathfrak{d}'^{(\nu)}$ und $\mathfrak{D}'^{(\nu)}$ $(\mathfrak{f}'^{(1)} = \mathfrak{d}'^{(1)} = \mathfrak{D}'^{(1)} = 1)$ bezeichnet. Unser Satz wird bewiesen sein, wenn wir

$$\mathfrak{f}_{\mathfrak{P}_1}'^{(\nu)} = \mathfrak{P}_1^{\lambda_\nu' + 1}$$

gezeigt haben. Sei dies für $\nu = k$ schon bewiesen. Wegen $\mathfrak{D}^{(k+1)} = \mathfrak{D}^{(1)} \mathfrak{D}'^{(k+1)}$ ist

$$\mathfrak{D}_{\mathfrak{P}_{k+1}}'^{(k+1)} = \mathfrak{P}_{k+1}^A \text{ mit } A = \sum_{i=1}^{k+1} (p^i - p^{i-1})(M_i + 1) - p^k(p-1)(M_1 + 1)$$

---

[6]) Man kann umgekehrt direkt die Differente von Z_n/K berechnen und so zu einem neuen Beweis der Führer-Diskriminantenformel kommen. Dies geschieht durch Berechnung des Führers von Z_n/Z_1. Doch treten dabei Fallunterscheidungen auf, die den Beweis unschön gestalten.

und $\mathfrak{d}_{\mathfrak{P}_1}^{\prime(k+1)} = \mathfrak{P}_1^A$. Nun ist

$$\begin{aligned} A &= \sum_{i=2}^{k+1} pM_i(p^{i-1} - p^{i-2}) - (p-1)(p^k - 1)M_1 + \sum_{i=2}^{k+1}(p^{i-1} - p^{i-2}) \\ &= \sum_{i=2}^{k+1}(pM_i - (p-1)M_1 + 1)(p^{i-1} - p^{i-2}) \\ &= \sum_{i=2}^{k+1}(\lambda_i' + 1)\varphi(p^{i-1}). \end{aligned}$$

Der Vergleich mit dem Führer-Diskriminantensatz, angewandt auf Z_{k+1}/Z_1,

$$\mathfrak{d}_{\mathfrak{P}_1}^{\prime(k+1)} = \prod_{i=2}^{k+1} \mathfrak{f}_{\mathfrak{P}_1}^{\prime(i)\varphi(p^{i-1})}$$

ergibt unter Berücksichtigung der Induktionsannahme die Richtigkeit unserer Behauptung für $\nu = k+1$.

4. Zur Bestimmung des *Geschlechtes* G von Z_n setzen wir voraus, daß Z_n den Körper k (und nicht eine echte algebraische Erweiterung von k) zum genauen Konstantenkörper besitzt. Dafür ist notwendig und hinreichend, daß die erzeugenden Gleichungen $\wp\theta = \beta$ absolut irreduzibel (d. h. auch bei Erweiterung von k auf die algebraisch abgeschlossene Hülle $\bar{k}$ irreduzibel) sind. Dafür genügt es wieder, vorauszusetzen, daß die erste Komponente der Vektorgleichung, $\wp\theta_1 = \beta_1$, in $\bar{K} = K\bar{k}$ irreduzibel ist. Die Bedingung dafür lautet, daß $\beta_1 \neq b + \wp\gamma$ mit b aus k und γ aus K ist. Unter dieser Voraussetzung ist

$$G = p^n g + \bar{g},$$

wo g das Geschlecht von K und $\bar{g}$ das Relativgeschlecht von Z_n/K bedeutet. Bezeichnet d den Grad der Diskriminante $\mathfrak{d}^{(n)}$, so ist $\bar{g} = \frac{d}{2} - (p^n - 1)$. f_i sei der Grad von $\mathfrak{f}_i$ $(i = 1, \ldots, n)$. Wegen $d = \sum_{i=1}^{n} \varphi(p^i) f_i$ ist also

$$G - 1 = p^n(g-1) + \tfrac{1}{2}\sum_{i=1}^{n} \varphi(p^i) f_i.$$

Diese Formel erhält praktischen Wert für den Fall, daß K der rationale Funktionenkörper $(g = 0)$ ist, weil dann die Komponenten des Vektors β im Großen reduziert angenommen und daraus die Grade $\mathfrak{f}_i$ berechnet werden können.

Aus unserer Geschlechtsformel folgt, daß stets

$$G - 1 \geqq p^n(g-1)$$

ist und daß das Gleichheitszeichen nur dann gilt, wenn Z_n über K unverzweigt ist [7]).

Für den Fall $g = 0$ leiten wir aus der Geschlechtsformel noch eine weitere Ungleichung her:

Ist G_ν das Geschlecht des Körpers Z_ν, so gelten die Ungleichungen

$$G_{\nu+1} > p(G_\nu + 1) \qquad (\nu = 1, 2, \ldots). \tag{1}$$

[7]) Dies ist offenbar wegen der allgemeinen Gültigkeit der Hilbertschen Diskriminantenformel für beliebige algebraische Funktionenkörper L/K in folgender Form richtig:

Ist L/K separabel algebraisch vom Grade m und die erzeugende Gleichung absolut irreduzibel, so gilt für das Geschlecht G von L stets

$$G - 1 \geqq m(g-1).$$

Das Gleichheitszeichen gilt nur, wenn L/K unverzweigt ist.

Beweis. Aus der Führerformel entnehmen wir, daß für die Grade f_ν der Führer $\mathfrak{f}_\nu$ die Ungleichungen $f_{\nu+1} > f_\nu$, insbesondere $f_2 > \frac{p}{2} f_1 + 1$, bestehen. Also ist

$$G_{\nu+1} - pG_\nu = \frac{1}{2} \sum_{i=2}^{\nu} \varphi(p^{i+1}) (f_{i+1} - f_i) + \frac{1}{2} \varphi(p^2) f_2 - \frac{1}{2} (\varphi(p^2) - \varphi(p)) f_1 - (p-1)$$
$$> \frac{f_1}{2} \left(\frac{p^3}{2} - \frac{3p^2}{2} + 2p - 1 \right) + \frac{1}{2} (p^2 - 3p + 2).$$

Nun muß, damit $G_1 > 0$ wird, $f_1 \geqq 3$ und für $p = 2$ sogar $f_1 \geqq 4$ sein. Daraus folgt dann $G_{\nu+1} - pG_\nu > p$, w. z. b. w.

5. Jetzt sei k algebraisch abgeschlossen und K als rationaler Funktionenkörper $K = k(x)$ darstellbar. Ein Primdivisor $\mathfrak{P}$ von Z_n heißt *Weierstraßpunkt* von Z_n, wenn $\dim \mathfrak{P}^{G_n} > 1$ ist, oder, was damit gleichbedeutend ist, wenn ein Element z aus Z_n mit der Divisorendarstellung $z \cong \frac{\mathfrak{G}}{\mathfrak{P}^\varrho}$ existiert, wo $\varrho \leqq G_n$ und $\mathfrak{G}$ ein ganzer Divisor ist. Wir wollen untersuchen, ob die Verzweigungspunkte zyklischer p-Körper stets Weierstraßpunkte sind.

Diese Frage können wir sofort bejahen, wenn $n \geqq 2$ ist. Denn ist $\mathfrak{P}_{n-1}$ der $\mathfrak{P}_n$ enthaltende Primdivisor von Z_{n-1} ($\mathfrak{P}_{n-1} = \mathfrak{P}_n^p$), so existiert jedenfalls ein Element z_{n-1} aus Z_{n-1} mit der Divisorendarstellung

$$z_{n-1} \cong \frac{\mathfrak{G}}{\mathfrak{P}_{n-1}^\sigma} = \frac{\mathfrak{G}}{\mathfrak{P}_n^{p\sigma}},$$

wobei $\sigma \leqq G_{n-1} + 1$. Nach (1) ist aber $p\sigma \leqq p(G_{n-1} + 1) < G_n$. Also ist $\mathfrak{P}_n$ Weierstraßpunkt in Z_n.

Wir brauchen nur noch den Fall $n = 1$ weiter zu verfolgen. Die im Großen reduzierte Form von β_1 sei

$$\beta_1 \cong \frac{\mathfrak{g}}{\mathfrak{p}_1^{\lambda^{(1)}} \cdots \mathfrak{p}_r^{\lambda^{(r)}}} \qquad (\lambda^{(i)}, p) = 1.$$

Dann ist $G_1 = (p-1)(\frac{1}{2} f_1 - 1)$ mit $f_1 = \sum_{i=1}^{r} (\lambda^{(i)} + 1)$. Es sei $\mathfrak{p}_i = \mathfrak{P}_i^p$ in Z_1. Nun unterscheiden wir zwei Fälle.

1. Fall: $G_1 \geqq p$. Für $\mathfrak{p}_i \neq \mathfrak{p}_\infty$ sei $x - \alpha_i \cong \frac{\mathfrak{p}_i}{\mathfrak{p}_\infty}$. Dann ist $\frac{1}{x - \alpha_i} \cong \frac{\mathfrak{g}}{\mathfrak{P}_i^p}$. Also ist $\mathfrak{P}_i$ Weierstraßpunkt. Falls $\mathfrak{p}_\infty$ unter den $\mathfrak{p}_i$ vorkommen sollte, nehmen wir $\frac{1}{x}$ statt $x - \alpha_i$, um $\mathfrak{P}_i$ als Weierstraßpunkt zu erkennen.

2. Fall: $1 < G_1 < p$. Dann ist notwendig $p > 2$. f_1 kann nur die Werte 3 und 4 annehmen.

Für $f_1 = 3$ muß β_1 notwendig von der Form $\beta_1 \cong \frac{\mathfrak{g}}{\mathfrak{p}_1^2}$ sein. Wegen $\theta_1 \cong \frac{\mathfrak{G}}{\mathfrak{P}_1^2}$ ist $\mathfrak{P}_1$ Weierstraßpunkt.

Für $f_1 = 4$ ist $G_1 = p - 1$. Entweder ist nun β_1 von der Form $\beta_1 \cong \frac{\mathfrak{g}}{\mathfrak{p}_1^3}$ (notwendig $p > 3$); dann ist $\mathfrak{P}_1$ wegen $\theta_1 \cong \frac{\mathfrak{G}}{\mathfrak{P}_1^3}$ Weierstraßpunkt.

Oder β_1 ist von der Form $\beta_1 \cong \frac{\mathfrak{g}}{\mathfrak{p}_1\mathfrak{p}_2}$ mit $\mathfrak{p}_1 \neq \mathfrak{p}_2$, also $\theta_1 \cong \frac{\mathfrak{G}}{\mathfrak{P}_1\mathfrak{P}_2}$. Es sei z ein Element aus K mit $z \cong \frac{\mathfrak{p}_1}{\mathfrak{p}_2}$. Dann ist $dw = \frac{dz}{z} \cong (\mathfrak{P}_1\mathfrak{P}_2)^{p-2}$ ein ganzes Differential in Z_1 [8]). Daher wird durch

$$dw,\ \theta dw,\ \ldots,\ \theta^{p-2}dw$$

ein vollständiges System linear unabhängiger ganzer Differentiale von Z_1 gegeben. Das allgemeine Differential von Z_1 hat also die Form

$$(c_0 + c_1\theta + \cdots + c_{p-2}\theta^{p-2})dw \qquad (c_i \text{ aus } k).$$

Daraus ist ersichtlich, daß die Verzweigungspunkte in diesem Falle keine Weierstraßpunkte sind.

Insgesamt haben wir jetzt folgenden Satz bewiesen:

Für einen zyklischen p-Körper des Grades p, der durch

$$\wp\theta_1 = \beta_1 \cong \frac{\mathfrak{g}}{\mathfrak{p}_1\mathfrak{p}_2} \quad (\mathfrak{p}_1 \neq \mathfrak{p}_2)$$

erzeugt wird, sind die Verzweigungspunkte keine Weierstraßpunkte. Dagegen sind in allen übrigen Fällen die Verzweigungspunkte zyklischer p-Körper, wenn ihr Geschlecht größer als 1 ist, zugleich Weierstraßpunkte dieser Körper.

---

[8]) Wegen $k(z) = k(x)$ ist

$$\frac{1}{z}dz \cong \frac{1}{z}\frac{\mathfrak{D}_x}{\mathfrak{N}_z^2} \cong \frac{\mathfrak{p}_2}{\mathfrak{p}_1}\frac{(\mathfrak{P}_1\mathfrak{P}_2)^{(p-1)(1+1)}}{\mathfrak{p}_2^2} = (\mathfrak{P}_1\mathfrak{P}_2)^{p-2}.$$

Eingegangen 10. August 1936.

Unverzweigte abelsche Körper vom Exponenten p^n über einem algebraischen Funktionenkörper der Charakteristik p.

Von *Hermann Ludwig Schmid* und *Ernst Witt* in Göttingen.

K sei ein algebraischer Funktionenkörper einer Unbestimmten vom Geschlecht g über einem algebraisch abgeschlossenen Konstantenkörper k der Charakteristik p. In einer kürzlich erschienenen Arbeit von H. Hasse und E. Witt [1]) wurde folgendes Ergebnis gewonnen:

Es existieren über K genau γ linear unabhängige zyklische Erweiterungskörper p-ten Grades, wobei γ als Rang einer gewissen invarianten Matrix eine der Zahlen 0 bis g ist.

Ist speziell k absolut algebraisch, so besagt dieses Resultat, wie wir zeigen werden: Es gibt genau p^γ Divisorenklassen C von K mit $C^p = 1$.

Wir verallgemeinern in der vorliegenden Arbeit diese Ergebnisse auf beliebigen Grad p^n ($n \geqq 1$). Neben dem selbständigen Interesse, welches das vergleichende Studium der unverzweigten abelschen Körper einerseits und der Struktur der Divisorenklassengruppe endlicher Ordnung andererseits besitzt, hoffen wir, damit vielleicht einen kleinen Beitrag zur Lösung der Riemannschen Vermutung in Funktionenkörpern beliebigen Geschlechtes zu geben. Die Methode unserer Untersuchung entnehmen wir einer eben erschienenen Arbeit von E. Witt [2]). Wir gelangen zu folgenden Hauptsätzen:

I. *Der größte unverzweigte abelsche Erweiterungskörper vom Exponenten p^n über K hat den Grad $p^{n\gamma}$ und seine Gruppe ist vom Typus* $(p^n, p^n, \ldots, p^n)$. Dabei ist γ die oben erwähnte Zahl.

II. *Ist speziell k absolut algebraisch, so gibt es $p^{n\gamma}$ Divisorenklassen C von K mit $C^{p^n} = 1$. Die Gruppe dieser C ist vom Typus* $(p^n, p^n, \ldots, p^n)$.

Schließlich bemerken wir, daß γ genau dann kleiner als g ist, wenn es ein totales Differential in K (d. h. ein Differential einer Funktion aus K) gibt, das überall endlich ist — im klassischen Fall haben bekanntlich totale Differentiale stets Pole.

1. A sei eine n-reihige Matrix, b ein n-gliedriger Vektor aus einem algebraisch abgeschlossenen Körper k der Charakteristik p. Wir behaupten folgenden Satz:

---

[1]) H. Hasse und E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p, Mh. Math. Phys. **43** (1936). — Diese Arbeit zitieren wir mit H.-W.

[2]) E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, dieser Band, S. 126.

Das Gleichungssystem

$$A x^p - x = b \tag{1}$$

hat stets eine Lösung.

Beweis. Simultane Transformationen $\overline{A} = SAS^{-p}$, $\overline{x} = Sx$, $\overline{b} = Sb$ mit einer regulären Matrix S aus k führen (1) in

$$\overline{A}\overline{x}^p - \overline{x} = \overline{b} \tag{1a}$$

über [3]). Nach H.-W. kann durch passende Wahl von S stets erreicht werden, daß $\overline{A}$ oberhalb der Hauptdiagonale lauter Nullen hat. Man sieht sofort, daß sich $\overline{x}_1, \ldots, \overline{x}_n$ durch Auflösung von algebraischen Gleichungen so bestimmen lassen, daß $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n)$ das Gleichungssystem (1 a) befriedigt.

2. Nun sei K ein algebraischer Funktionenkörper einer Unbestimmten über einem algebraisch abgeschlossenen Konstantenkörper k der Charakteristik p. K habe das Geschlecht g.

An jeder Primstelle $\mathfrak{p}$ sei ein Element $\gamma^{\mathfrak{p}}$ aus der $\mathfrak{p}$-adischen Erweiterung $K_{\mathfrak{p}}$ vorgegeben, und zwar sollen unter diesen Elementen nur für endlich viele Stellen $\mathfrak{p}$ Hauptteile in der Entwicklung auftreten. Unter diesen Voraussetzungen beweisen wir den Satz:

Die Gleichungen

$$\xi + \wp\xi^{\mathfrak{p}} = \gamma^{\mathfrak{p}} \tag{2}$$

lassen sich mit Elementen $\xi^{\mathfrak{p}}$ aus $K_{\mathfrak{p}}$ und einem Element ξ aus K lösen.

Beweis. Wir dürfen jedes $\gamma^{\mathfrak{p}}$ um dasselbe Element α aus K abändern. Diese Abänderungsmöglichkeit benutzen wir, um die $\gamma^{\mathfrak{p}}$ geeignet zu normieren.

Es sei $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ wie in H.-W. ein reguläres Primdivisorensystem, d. h. $\dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g) = 1$. Für eine Primstelle $\mathfrak{p} \neq \mathfrak{p}_i$, für welche $\gamma^{\mathfrak{p}}$ den Nenner $\mathfrak{p}^r$ $(r > 0)$ hat, können wir ein α aus K so bestimmen, daß $\gamma^{\mathfrak{p}} - \alpha$ höchstens den Nenner $\mathfrak{p}^{r-1}$ hat und im übrigen nur die Hauptteile von $\gamma^{\mathfrak{p}_i} - \alpha$ $(i = 1, \ldots, g)$ verändert werden. Weil nämlich

$$\dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}^r) - \dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}^{r-1}) = 1$$

ist, so gibt es ein Element α aus K, welches bei $\mathfrak{p}$ den genauen Nenner $\mathfrak{p}^r$ mit einem beliebig vorgeschriebenen Anfangskoeffizienten hat und sonst nur noch Pole an den Stellen $\mathfrak{p}_i$ besitzt. Nach dieser schrittweisen Abänderung besitzen die $\gamma^{\mathfrak{p}}$ höchstens noch an den Stellen $\mathfrak{p}_i$ $(i = 1, \ldots, g)$ Pole.

Hat $\gamma^{\mathfrak{p}_i}$ den Nenner $\mathfrak{p}_i^{r_i}$ $(r_i > 1)$, so können wir $\gamma^{\mathfrak{p}_i}$ wieder um ein Element α aus K so abändern, daß $\gamma^{\mathfrak{p}_i} - \alpha$ einen kleineren Nenner erhält, während sich an den Stellen $\mathfrak{p}_j$ $(j \neq i)$ die Hauptteile höchstens in den Gliedern erster Ordnung verändern und $\gamma^{\mathfrak{p}} - \alpha$ $(\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_g)$ nach wie vor keine Nenner hat. Wegen

$$\dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}_i^{r_i}) - \dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}_i^{r_i-1}) = 1$$

gibt es nämlich ein Element α aus K, das an der Stelle $\mathfrak{p}_i$ den genauen Nenner $\mathfrak{p}_i^{r_i}$ mit passendem Anfangskoeffizenten besitzt und sonst höchstens noch an den Stellen $\mathfrak{p}_j$ $(j \neq i)$ Pole erster Ordnung hat.

---

[3]) Unter S^p verstehen wir die Matrix, die aus S durch Potenzierung aller Elemente mit p entsteht. S^p ist also nicht etwa die p-te Potenz im Sinne des Matrizenprodukts; diese wird gar nicht vorkommen.

Damit haben wir erreicht, daß die neuen $\gamma^{\mathfrak{p}_i}$ $(i = 1, \ldots, g)$ höchstens den Nenner $\mathfrak{p}_i$ haben, während die übrigen $\gamma^{\mathfrak{p}}$ $(\mathfrak{p} \neq \mathfrak{p}_i)$ ganz sind.

Es sei $\pi_1, \ldots, \pi_g$ ein System von Primelementen an den Stellen $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$. Nach H.-W. existieren Elemente $v_1, \ldots, v_g$ aus K, welche die Entwicklungen

$$v_j = \frac{e_{ij}}{\pi_i^p} - \frac{a_{ij}}{\pi_i} + \cdots \qquad (i, j = 1, \ldots, g) \tag{3}$$

haben und an den übrigen Stellen ganz sind. Weiter sei

$$\gamma^{\mathfrak{p}_i} = \frac{b_i}{\pi_i} + \cdots$$

und $x = (x_1, \ldots, x_g)$ eine Lösung der Matrizengleichung

$$A x^p - x = b,$$

wobei $A = (a_{ij})$ und $b = (b_i)$ gesetzt ist. Bilden wir das Element

$$\xi = \sum_{j=1}^{g} v_j x_j^p$$

aus K, so wird $\gamma^{\mathfrak{p}_i} + \xi + \wp\frac{x_i}{\pi_i}$ ganz. Für die übrigen Stellen $\mathfrak{p} \neq \mathfrak{p}_i$ bleibt $\gamma^{\mathfrak{p}} + \xi$ ganz. Also ist in jedem Falle

$$\gamma^{\mathfrak{p}} + \xi = \wp\xi^{\mathfrak{p}}.$$

3. Wir betrachten im Sinne der Arbeit von E. Witt[2]) Vektoren $(\alpha_1, \ldots, \alpha_n)$ mit Elementen aus K. Es handelt sich also nicht etwa um gewöhnliche lineare Vektoren; diese werden von nun an nicht mehr vorkommen. Wir nennen einen solchen Vektor **zerfallend,** wenn

$$(\alpha_1, \ldots, \alpha_n) = \wp(\beta_1, \ldots, \beta_n)$$

mit Elementen $\beta_1, \ldots, \beta_n$ aus K ist. Wir nennen $(\alpha_1, \ldots, \alpha_n)$ **unverzweigt,** wenn an jeder Stelle

$$(\alpha_1, \ldots, \alpha_n) = \wp(\beta_1^{\mathfrak{p}}, \ldots, \beta_n^{\mathfrak{p}})$$

mit Elementen $\beta_1^{\mathfrak{p}}, \ldots, \beta_n^{\mathfrak{p}}$ aus $K_{\mathfrak{p}}$ ist. Es gilt folgender

Erweiterungssatz. *Jeder unverzweigte Vektor* $(\alpha_1, \ldots, \alpha_{n-1})$ *läßt sich zu einem unverzweigten Vektor* $(\alpha_1, \ldots, \alpha_{n-1}, \xi)$ *fortsetzen.*

Beweis. Nach Voraussetzung ist für jede Stelle $\mathfrak{p}$

$$(\alpha_1, \ldots, \alpha_{n-1}) = \wp(\beta_1^{\mathfrak{p}}, \ldots, \beta_{n-1}^{\mathfrak{p}}).$$

Man sieht sofort durch Induktion nach n: An denjenigen Stellen, an denen die α_ν ganz sind, müssen auch die $\beta_\nu^{\mathfrak{p}}$ ganz sein. Das Gleichungssystem

$$(\alpha_1, \ldots, \alpha_{n-1}, \xi) = \wp(\beta^{\mathfrak{p}}, \ldots, \beta_{n-1}^{\mathfrak{p}}, \xi^{\mathfrak{p}})$$

ist gleichwertig mit einem System

$$\xi - \wp\xi^{\mathfrak{p}} = \gamma^{\mathfrak{p}},$$

wo die $\gamma^{\mathfrak{p}}$ ganz rational von den α_ν und $\beta_\nu^{\mathfrak{p}}$ abhängen, folglich nur für endlich viele Stellen $\mathfrak{p}$ Hauptteile besitzen. In **2** haben wir die Lösbarkeit eines solchen Systems schon nachgewiesen.

4. Bezeichnen wir zerfallende bzw. unverzweigte Vektoren der Länge n mit $\mathfrak{z}_n$ bzw. $\mathfrak{u}_n$, so folgt, ähnlich wie in der Kummerschen Theorie, daß der Gruppenindex $(\mathfrak{u}_n : \mathfrak{z}_n)$ gleich dem Grad des größten abelschen unverzweigten Körpers vom Exponenten p^n ist.

Für die Matrix $A = (a_{ij})$ aus (3) sei γ der Rang von $AA^p \cdots A^{p^{\vartheta-1}}$. In H.-W. wurde festgestellt, daß der größte abelsche unverzweigte Körper vom Exponenten p den Grad p^γ hat. Wir behaupten hier folgenden Satz:

Der größte abelsche unverzweigte Körper vom Exponenten p^n hat den Grad $p^{n\gamma}$.

Beweis. Es sei A eine Gruppe und B eine Untergruppe. T sei eine homomorphe Abbildung, bei welcher genau die Untergruppen A_1 bzw. B_1 in 1 übergehen mögen. Dann gilt

$$(A : B) = (TA : TB) \cdot (A_1 : B_1).$$

Dieses gruppentheoretische Prinzip wenden wir auf $(\mathfrak{u}_n : \mathfrak{z}_n)$ an. Unter T verstehen wir Weglassung der letzten Komponente. Dabei geht nach unserem Erweiterungssatz $\mathfrak{u}_n$ in jeden beliebigen Vektor $\mathfrak{u}_{n-1}$ über; es ist klar, daß dabei $\mathfrak{z}_n$ in jeden beliebigen Vektor $\mathfrak{z}_{n-1}$ übergeht. Streichen wir bei denjenigen Vektoren, die bei unserer Abbildung in Null übergehen, die vorderen $n-1$ Nullen, so entstehen gerade die Gruppen $\mathfrak{u}_1$ bzw. $\mathfrak{z}_1$. Also gilt

$$(\mathfrak{u}_n : \mathfrak{z}_n) = (\mathfrak{u}_{n-1} : \mathfrak{z}_{n-1}) \cdot (\mathfrak{u}_1 : \mathfrak{z}_1). \tag{4}$$

Nach H.-W. ist $(\mathfrak{u}_1 : \mathfrak{z}_1) = p^\gamma$. Durch Induktion sei schon gezeigt, daß $(\mathfrak{u}_{n-1} : \mathfrak{z}_{n-1}) = p^{(n-1)\gamma}$ ist. Aus (4) folgt dann

$$(\mathfrak{u}_n : \mathfrak{z}_n) = p^{n\gamma},$$

w. z. b. w.

5. Wir beweisen folgende **Hauptsätze:**

I. *Die Gruppe $\mathfrak{A}_n$ des größten abelschen unverzweigten Körpers vom Exponenten p^n über K ist direktes Produkt von zyklischen Gruppen der Ordnung p^n.*

II. *Ist speziell k absolut algebraisch, so hat die Gruppe der Divisorenklassen vom Exponenten p^n den Grad $p^{n\gamma}$ und ist Produkt von γ zyklischen Gruppen der Ordnung p^n.*

Wir schicken folgende allgemeine gruppentheoretische Bemerkung voraus: Jede abelsche Gruppe $\mathfrak{A}$ mit endlich vielen Erzeugenden ist als freie abelsche Gruppe mit den Erzeugenden

$$x_1, \ldots, x_r; \quad y_1, \ldots, y_s; \quad z_1, \ldots, z_t$$

und den definierenden Relationen

$$y_i^{p^{\nu_i}} = 1, \quad z_i^{e_i} = 1 \qquad (e_i \not\equiv 0 \bmod p)$$

darstellbar. Die Elemente x_i sind von unendlicher Ordnung. In diesen Bezeichnungen ist die

Ordnung der größten Faktorgruppe $\mathfrak{A}_1$ vom Exponenten p gleich

$$p^{r+s}$$

und die

Ordnung der größten Faktorgruppe $\mathfrak{A}_n$ vom Exponenten p^n gleich

$$p^{nr + \sum_{\nu_i \leqq n} n + \sum_{\nu_i < n} \nu_i}. \tag{5}$$

Beweis von **I.** $\mathfrak{A} = \mathfrak{A}_n$ sei die galoissche Gruppe des größten abelschen unverzweigten Körpers vom Exponenten p^n. Es folgt $r = 0$ und $t = 0$ und alle $\nu_i \leqq n$. Da $\mathfrak{A}_1$ die Ordnung p^γ hat, ist $s = \gamma$. Da $\mathfrak{A}_n$ die Ordnung $p^{n\gamma}$ hat, folgt $\nu_i \geqq n$, also alle $\nu_i = n$, w. z. b. w.

Beweis von **II.** Es sei $K = k(x, y)$ mit der erzeugenden Gleichung $f(x, y) = 0$. Ferner sei

$$(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}) \qquad (i = 1, \ldots, p^{n\gamma})$$

ein Vertretersystem der unverzweigten Vektoren modulo den zerfallenden Vektoren. k' sei ein endlicher Körper, der

1. die Koeffizienten von f

2. die Koeffizienten von $\alpha_k^{(i)}$ in ihrer Darstellung als rationale Ausdrücke in x und y

enthält. Wir setzen $K' = k'(x, y)$. K_n' sei der größte abelsche unverzweigte Körper vom Exponenten p^n über K'. Dann ergeben sich die in nachstehender Zeichnung angeführten Körper.

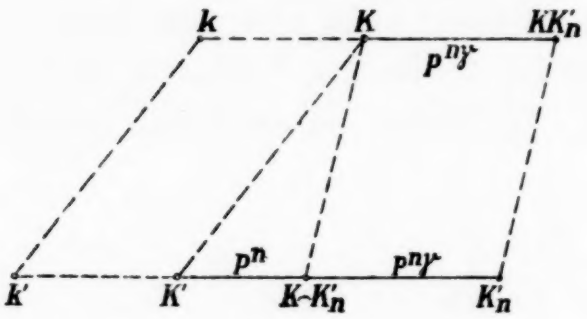

Fig. 1.

Dabei ist das Kompositum KK_n' der größte abelsche unverzweigte Körper vom Exponenten p^n über K und der Durchschnitt $K \cap K_n'$ der größte unverzweigte Körper, der aus K' durch Konstantenerweiterung entsteht; er hat über K' den Grad p^n.

Jetzt sei $\mathfrak{A}$ die Divisorenklassengruppe von K', also $r = 1$ und daher $s = \gamma$. Nach der Klassenkörpertheorie hat $\mathfrak{A}_1$ die Ordnung $p^{\gamma+1}$ und $\mathfrak{A}_n$ die Ordnung $p^{n(\gamma+1)}$ [4]). Ein Vergleich mit (5) ergibt $\nu_i \geqq n$. Daher wird die in $\mathfrak{A}$ größte Untergruppe $\mathfrak{U}_n$ vom Exponenten p^n von den Elementen $y_i^{\nu_i - n}$ erzeugt. $\mathfrak{U}_n$ hat die Ordnung $p^{n\gamma}$ und ist vom Typus $(p^n, p^n, \ldots, p^n)$.

Nun kann $\mathfrak{U}_n$ bei Erweiterung von k' zu k nicht größer werden. Einerseits läge nämlich jede etwa neu hinzukommende Divisorenklasse schon in einer endlichen Konstantenerweiterung von K'. Andererseits erfüllt auch eine endliche Erweiterung k'' von k' die an k' gestellten Forderungen und führt daher zur selben Anzahl $p^{n\gamma}$. Es kann also keine neue Divisorenklasse hinzukommen. Also ist $\mathfrak{U}_n$ gleich der gesuchten Gruppe in K.

Insbesondere ist damit für $n = 1$ die in der Einleitung erwähnte Ergänzung der Arbeit H.-W. hinsichtlich Divisorenklassen der Ordnung p bewiesen.

6. Wir beweisen den Satz:

Es gibt $g - \varrho$ linear unabhängige überall endliche totale Differentiale in K, wobei ϱ der Rang der Matrix $A = (a_{ij})$ ist.

Es sei $d\alpha$ ein totales überall endliches Differential in K. Wir dürfen α additiv um eine p-te Potenz aus K abändern. Wir zeigen dann, daß wir infolge dieser Abänderungsmöglichkeit α stets in die Form

$$\alpha = \sum_{j=1}^{g} c_j v_j \qquad (c_j \text{ aus } k) \tag{6}$$

mit den in (3) eingeführten Elementen v_j bringen können.

---

[4]) E. Witt, Der Existenzsatz für abelsche Funktionenkörper, Journ. f. Math. **173** (1935).

Zunächst beseitigen wir analog wie oben in **2** die Hauptteile von α an den Stellen $\mathfrak{p} \neq \mathfrak{p}_i$ auf Kosten der Hauptteile an den Stellen $\mathfrak{p}_i$ $(i = 1, \ldots, g)$. Dann sorgen wir dafür, daß α höchstens den Nenner $(\mathfrak{p}_1 \cdots \mathfrak{p}_g)^p$ hat. Weil $d\alpha$ keine Hauptteile besitzt, muß an den Stellen $\mathfrak{p}_i$ des regulären Systems

$$\alpha \equiv \frac{c_i}{\pi_i^p} \bmod \mathfrak{p}_i^0$$

sein. Dann hat aber die Differenz

$$\alpha - \sum_{j=1}^{g} c_j v_j$$

höchstens den Nenner $\mathfrak{p}_1 \cdots \mathfrak{p}_g$, ist also konstant. Also können wir α tatsächlich in die Form (6) bringen.

Damit nun

$$\frac{d\alpha}{d\pi_i} = \frac{d}{d\pi_i} \sum_j c_j v_j \equiv \sum_j \frac{a_{ij} c_j}{\pi_i^2} \bmod \mathfrak{p}_i^0$$

ganz ist, muß

$$\sum_{j=1}^{g} a_{ij} c_j = 0$$

sein. Dies trifft für $g - \varrho$ unabhängige α zu.

Verschiedene α von der Form (6) liefern aber verschiedene Differentiale. Denn aus $d\alpha = 0$ folgt $\alpha = \beta^p$ mit β aus K [4]). β hat dann höchstens den Nenner $\mathfrak{p}_1 \cdots \mathfrak{p}_g$, ist also konstant; also ist auch α konstant und dann nach (6) notwendig $\alpha = 0$.

Die in der Einleitung erwähnte Tatsache ergibt sich daraus, daß für γ als Rang von $AA^p \cdots A^{p^{g-1}}$ stets $\gamma \leqq \varrho$ gilt und daß aus $\varrho = g$ auch $\gamma = g$ folgt.

Eingegangen 29. August 1936.

Die Gruppe der p^n-primären Zahlen für einen Primteiler $\mathfrak{p}$ von p.

Von *Helmut Hasse* in Göttingen.

In meinem Zahlbericht, Teil II, § 9, mußte ich die Frage nach einer Kongruenzcharakterisierung der p^n-primären Zahlen für einen Primteiler $\mathfrak{p}$ von p offen lassen. Ich gebe nachstehend eine solche Charakterisierung. Diese stützt sich einerseits auf die Einführung eines erweiterten Potenzbegriffs, der seine Grundlegung in der Strukturtheorie der diskret bewerteten perfekten Körper findet [1]), andrerseits auf die Theorie der zyklischen Erweiterungen vom Grade p^n bei Charakteristik p [2]). Diesen neueren Untersuchungen entsprechend behandle ich die Frage gleich allgemeiner, als es für die Anwendung auf algebraische Zahlkörper erforderlich ist.

1.

Sei l ein diskret bewerteter perfekter Körper der Charakteristik 0 mit vollkommenem Restklassenkörper $\mathfrak{k}$ der Primzahlcharakteristik p. Nach der angeführten Strukturtheorie ist l eine voll-verzweigte (Eisensteinsche) Erweiterung endlichen Grades eines eindeutig bestimmten perfekten unverzweigten Teilkörpers k mit demselben Restklassenkörper $\mathfrak{k}$.

Zu jedem gegebenen vollkommenen Restklassenkörper $\mathfrak{k}$ der Charakteristik p existiert genau ein diskret bewerteter perfekter unverzweigter Körper k der Charakteristik 0, bestehend aus allen Reihen

$$\alpha = \sum_{\nu=\nu_0}^{\infty} \alpha_\nu\, p^\nu$$

mit Koeffizienten α_ν aus einem $\mathfrak{k}$ multiplikationstreu zugeordneten Repräsentantensystem und mit einer durch $\mathfrak{k}$ eindeutig bestimmten Additionsvorschrift. Jeder Automorphismus S von $\mathfrak{k}$ überträgt sich zunächst auf das multiplikationstreue Repräsentantensystem und dann in der Form

$$\alpha^S = \sum_{\nu=\nu_0}^{\infty} \alpha_\nu^S\, p^\nu$$

[1]) Siehe H. Hasse und F. K. Schmidt, Die Struktur diskret bewerteter Körper, Journ. f. Math. **170** (1934), 4—63. Eine neue einfachere Begründung dieser Theorie gab kürzlich O. Teichmüller, Über die Struktur diskret bewerteter perfekter Körper, Göttinger Nachrichten (Neue Folge) I **1** (1936), 151—161; eine ausführliche Darstellung des hier in Frage kommenden, auf vollkommene Restklassenkörper bezüglichen Teils dieser Arbeit gibt E. Witt in der in diesem Heft, S. 126—140, erscheinenden Arbeit: Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, auf die ich mich hier ohne weitere Einzelverweise beziehen werde.

[2]) Siehe schon A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Amer. Math. Soc. **40** (1934), 625—631; E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^l, Journ. f. Math. **174** (1936), 237—245. Eine neue, für den Zweck dieser Arbeit besonders brauchbare Begründung gibt Witt in der unter [1]) genannten Arbeit.

auf k. k enthält insbesondere den dem Primkörper $\mathfrak{k}_0$ der Charakteristik p zugeordneten Teilkörper k_0 der Charakteristik 0, den Körper der p-adischen Zahlen.

Für Einseinheiten, d. h. Elemente aus l der Form $1-\xi$ mit $\xi \equiv 0 \bmod \mathfrak{p}$, wo $\mathfrak{p}$ das Primideal von l bezeichnet, sind in bekannter Weise die Potenzen $(1-\xi)^a$ mit ganzen Exponenten a aus dem p-adischen Zahlkörper k_0 erklärt, nämlich als

$$(1-\xi)^a = \sum_{\nu=0}^{\infty} (-1)^\nu \binom{a}{\nu} \xi^\nu,$$

und es gelten dafür die Regeln:

$$(1_0) \qquad (1-\xi)^a \equiv 1 - a\xi \bmod \xi^2,$$

$$(2_0) \qquad (1-\xi)^a (1-\xi)^b = (1-\xi)^{a+b},$$

$$(3_0) \qquad ((1-\xi)^a)^b = (1-\xi)^{ab},$$

$$(4_0) \qquad (1-\xi_1)^a (1-\xi_2)^a = ((1-\xi_1)(1-\xi_2))^a.$$

Ich will diesen Potenzbegriff auf ganze Exponenten α aus dem unverzweigten Teilkörper k von l erweitern.

Dazu gehe ich aus von der für $\eta \equiv 0 \bmod \mathfrak{p}$ aus l konvergenten Logarithmusreihe

$$-\log(1-\eta) = \sum_{n=1}^{\infty} \frac{\eta^n}{n}.$$

Diese spalte ich unter Einführung der ebenfalls für $\eta \equiv 0 \bmod \mathfrak{p}$ konvergenten Reihe

$$L(1-\eta) = \sum_{\varrho=0}^{\infty} \frac{\eta^{p^\varrho}}{p^\varrho}$$

folgendermaßen auf:

$$-\log(1-\eta) = \sum_{(m,p)=1} \frac{1}{m} L(1-\eta^m).$$

Durch Umkehrung mittels der Möbiusschen μ-Funktion ergibt sich daraus

$$\begin{aligned} L(1-\eta) &= -\sum_{(m,p)=1} \frac{\mu(m)}{m} \log(1-\eta^m) \\ &= -\sum_{(m,p)=1} \log(1-\eta^m)^{\frac{\mu(m)}{m}} \\ &= -\log \prod_{(m,p)=1} (1-\eta^m)^{\frac{\mu(m)}{m}} \\ &= -\log P(1-\eta), \end{aligned}$$

wo

$$P(1-\eta) = \prod_{(m,p)=1} (1-\eta^m)^{\frac{\mu(m)}{m}}$$

gesetzt ist; dies Produkt konvergiert ebenfalls für $\eta \equiv 0 \bmod \mathfrak{p}$. Es besitzt eine Potenzreihenentwicklung

$$P(1-\eta) = 1 - \eta - c_2\eta^2 - c_3\eta^3 - \cdots$$

mit ganzen p-adischen Koeffizienten $c_2, c_3, \ldots$ Daher läßt sich die Beziehung

$$1-\xi = P(1-\eta)$$

im Bereich der $\xi \equiv 0 \bmod \mathfrak{p}$ aus l eindeutig umkehren, und zwar in der Form

$$1-\eta = Q(1-\xi),$$

wo

$$Q(1-\xi) = 1 - \xi - d_2\xi^2 - d_3\xi^3 - \cdots$$

mit ganzen p-adischen Koeffizienten $d_2, d_3, \ldots$ ist. Durch die Relationen

$$1 - \xi = P(1-\eta), \quad 1 - \eta = Q(1-\xi)$$

wird also eine umkehrbar eindeutige Abbildung der Gruppe der Einseinheiten von l auf sich geliefert, bei der überdies

$$1 - \xi \equiv 1 - \eta \bmod. (\xi^2 \sim \eta^2)$$

gilt. Dabei ist nach obigem

$$-\log(1-\xi) = L(1-\eta);$$

die Abbildung bewirkt also, daß die Logarithmusreihe

$$-\log(1-\xi) = \sum_{n=1}^{\infty} \frac{\xi^n}{n}$$

in die einfachere Reihe

$$L(1-\eta) = \sum_{\varrho=0}^{\infty} \frac{\eta^{p^\varrho}}{p^\varrho}$$

übergeführt wird [3]).

Ich definiere nun für beliebige $\xi \equiv 0 \bmod. \mathfrak{p}$ aus l und beliebige ganze

$$\alpha = \sum_{\nu=0}^{\infty} \alpha_\nu p^\nu$$

aus k (in ihrer eindeutigen Entwicklung nach multiplikationstreuen Repräsentanten α_ν von $\mathfrak{k}$ in k) die Potenz $(1-\xi)^\alpha$ durch

$$(1-\xi)^\alpha = \prod_{\nu=0}^{\infty} (P(1-\alpha_\nu\eta))^{p^\nu},$$

wo η zu ξ aus

$$P(1-\eta) = 1 - \xi, \quad \text{also} \quad Q(1-\xi) = 1 - \eta$$

bestimmt ist. Ich beweise dann die Gültigkeit der folgenden Regeln:

(1) $$(1-\xi)^\alpha \equiv 1 - \alpha\xi \bmod. \xi^2,$$

(2) $$(1-\xi)^\alpha (1-\xi)^\beta = (1-\xi)^{\alpha+\beta},$$

(3) $$((1-\xi)^\alpha)^a = (1-\xi)^{a\alpha} \quad \text{für ganze } a \text{ aus } k_0,$$

sowie das Übereinstimmen des erweiterten Potenzbegriffs mit dem oben angeführten speziellen für ganze $\alpha = a$ aus k_0.

Die Gültigkeit von (1) ergibt sich ohne weiteres aus dem oben über die Funktionen P, Q Gesagten. Danach ist nämlich

$$P(1-\alpha_\nu\eta) \equiv 1 - \alpha_\nu\eta \equiv 1 - \alpha_\nu\xi \bmod. \xi^2,$$

also

$$(P(1-\alpha_\nu\eta))^{p^\nu} \equiv (1-\alpha_\nu\xi)^{p^\nu} \equiv 1 - \alpha_\nu p^\nu \xi \bmod. \xi^2$$

(daß dies $\equiv 1 \bmod. \xi^2$ für $\nu \geqq 1$ ist, brauchen wir nicht), und somit in der Tat

$$(1-\xi)^\alpha \equiv \prod_{\nu=0}^{\infty} (1-\alpha_\nu p^\nu \xi) \equiv 1 - \sum_{\nu=0}^{\infty} \alpha_\nu p^\nu \cdot \xi = 1 - \alpha\xi \bmod. \xi^2.$$

---

[3]) Dieser Formalismus wurde bereits mit Vorteil angewandt in E. Artin und H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln, Abh. Math. Seminar Hamburg **6** (1928), 151f.

Zum Beweise von (2) und (3) zeige ich zunächst die Gleichheit der Logarithmen beider Seiten. Es ist nach obigem

$$\begin{aligned}
-\log((1-\xi)^{\alpha}) &= -\sum_{\nu=0}^{\infty} p^{\nu} \log P(1-\alpha_{\nu}\eta) \\
&= \sum_{\nu=0}^{\infty} p^{\nu} L(1-\alpha_{\nu}\eta) \\
&= \sum_{\nu=0}^{\infty} p^{\nu} \sum_{\varrho=0}^{\infty} \frac{\alpha_{\nu}^{p^{\varrho}} \eta^{p^{\varrho}}}{p^{\varrho}} \\
&= \sum_{\varrho=0}^{\infty} \left(\sum_{\nu=0}^{\infty} \alpha_{\nu}^{p^{\varrho}} p^{\nu} \right) \frac{\eta^{p^{\varrho}}}{p^{\varrho}} \\
&= \sum_{\varrho=0}^{\infty} \frac{\alpha^{P^{\varrho}} \eta^{p^{\varrho}}}{p^{\varrho}},
\end{aligned}$$

wo die

$$\alpha^{P^{\varrho}} = \sum_{\nu=0}^{\infty} \alpha_{\nu}^{p^{\varrho}} p^{\nu}$$

aus

$$\alpha = \sum_{\nu=0}^{\infty} \alpha_{\nu} p^{\nu}$$

durch die oben besprochene Übertragung der Automorphismen $P^{\varrho} = (\mathfrak{k} \to \mathfrak{k}^{p^{\varrho}})$ des Restklassenkörpers $\mathfrak{k}$ auf den Körper k entstehen. Wegen der Automorphieeigenschaft hat man einerseits

$$\alpha^{P^{\varrho}} + \beta^{P^{\varrho}} = (\alpha+\beta)^{P^{\varrho}}$$

und daraus

$$\log((1-\xi)^{\alpha}(1-\xi)^{\beta}) = \log((1-\xi)^{\alpha}) + \log((1-\xi)^{\beta}) = \log((1-\xi)^{\alpha+\beta}),$$

andrerseits, da k_0 wie $\mathfrak{k}_0$ bei den P^{ϱ} elementweise festbleibt,

$$a\alpha^{P^{\varrho}} = (a\alpha)^{P^{\varrho}}$$

und daraus

$$\log(((1-\xi)^{\alpha})^{a}) = a\log((1-\xi)^{\alpha}) = \log((1-\xi)^{a\alpha}).$$

Um aus der Gleichheit der Logarithmen in (2) und (3) auf das Bestehen von (2) und (3) selbst zurückzuschließen, fasse man ξ als eine Unbestimmte auf, so daß es sich um Potenzreihen $\sum_{\nu} \gamma_{\nu}\xi^{\nu}$ mit Koeffizienten γ_{ν} aus k handelt. Nennt man eine solche Potenzreihe konvergent, wenn sie bei Einsetzung beliebiger über k algebraischer ξ von positiver p-adischer Ordnungszahl r p-adisch konvergiert (d. h. wenn $\sum_{\nu} \gamma_{\nu} p^{r\nu}$ für jedes positive rationale r p-adisch konvergiert), so sind unsere Formeln und Schlüsse wegen der Willkürlichkeit des Körpers l auch richtig im Sinne dieser allgemeineren Konvergenz. Sind dann $1-\xi_1, 1-\xi_2$ zwei Einheitspotenzreihen dieser Art, so kann natürlich aus $\log(1-\xi_1) = \log(1-\xi_2)$ auf $\xi_1 = \xi_2$ geschlossen werden. Da die linken und rechten Seiten in (2) und (3) Einheitspotenzreihen in ξ sind, ergibt sich also die Richtigkeit von (2) und (3) für unbestimmte ξ; diese Identitäten ergeben dann (2) und (3) für alle ξ positiver p-adischer Ordnungszahl aus l durch Einsetzung.

Für ganzes $\alpha = a$ aus k_0 wird wegen $a^{p^\varrho} = a$

$$-\log((1-\xi)^\alpha) = a\sum_{\varrho=0}^{\infty}\frac{\eta^{p^\varrho}}{p^\varrho} = aL(1-\eta) = -a\log(1-\xi) = -\log((1-\xi)^a),$$

wo die Potenz links im neu definierten Sinne, rechts im bisherigen Sinne verstanden ist. Daraus folgt ganz analog wie vorher das Übereinstimmen der beiden Potenzen selbst.

Es sei noch bemerkt, daß sich die Regeln (3_0) und (4_0) nicht auch zu entsprechenden Regeln für $((1-\xi)^\alpha)^\beta$ und $(1-\xi_1)^\alpha(1-\xi_2)^\alpha$ verallgemeinern lassen; insbesondere ist schon $((1-\xi)^a)^\alpha$ für ganze a aus k_0 im allgemeinen nicht gleich $(1-\xi)^{a\alpha}$, wie nachher noch direkt hervortreten wird. Das macht aber für die beabsichtigte Anwendung nichts aus.

2.

Nach der Strukturtheorie der diskret bewerteten perfekten Körper entsprechen sich die

$$\left\{\begin{array}{ccccc} \text{unverzweigten} & \text{Erweiterungskörper} & L & \text{von} & l \\ \text{,,} & \text{,,} & K & \text{,,} & k \\ \text{sämtlichen} & \text{,,} & \mathfrak{R} & \text{,,} & \mathfrak{k} \end{array}\right\}$$

gegenseitig eindeutig derart, daß

K der größte absolut-unverzweigte Teilkörper von L, also L/K voll-verzweigt,

$\mathfrak{R}$ der Restklassenkörper von K und L

ist, also analog wie eingangs die Grundkörper l, k, $\mathfrak{k}$ selbst, und es gilt dabei überdies

$$L = Kl, \quad k = K \frown l,$$

sowie im Falle galoisscher Erweiterungskörper

$$\text{Galoisgruppe } L/l \cong \text{Galoisgruppe } K/k \cong \text{Galoisgruppe } \mathfrak{R}/\mathfrak{k},$$

wobei die erstere Isomorphie durch den Verschiebungssatz der Galoisschen Theorie zustande kommt, die letztere durch die eingangs besprochene Übertragung der Automorphismen des Restklassenkörpers auf den zugehörigen absolut-unverzweigten Körper.

Insbesondere entsprechen sich so gegenseitig eindeutig die

$$\left\{\begin{array}{ccccccccc} \text{unverzweigten} & \text{zyklischen} & \text{Erweiterungskörper} & L & \text{vom} & \text{Grade} & m & \text{über} & l \\ \text{,,} & \text{,,} & \text{,,} & K & \text{,,} & \text{,,} & m & \text{,,} & k \\ \text{sämtlichen} & \text{,,} & \text{,,} & \mathfrak{R} & \text{,,} & \text{,,} & m & \text{,,} & \mathfrak{k} \end{array}\right\}.$$

Diese Zuordnung wollen wir im folgenden näher betrachten. Wir setzen dabei voraus, daß l die m-ten Einheitswurzeln enthält; eine primitive solche sei mit ζ bezeichnet. Ferner bezeichne S einen erzeugenden Automorphismus von L/l, sowie ohne Mißverständnis gleichzeitig die nach dem eben Gesagten zugeordneten erzeugenden Automorphismen von K/k und $\mathfrak{R}/\mathfrak{k}$.

L/l besitzt eine algebraisch ausgezeichnete Erzeugung, nämlich eine Erzeugung als Kummerscher Körper:

$$L = l(\Theta) \quad \text{mit} \quad \Theta^m = \omega, \qquad \omega \text{ in } l.$$

Dabei liegen Θ, ω bis auf beliebige Substitutionen

$$\Theta \to \Theta^\varkappa \alpha, \qquad \omega \to \omega^\varkappa \alpha^m \left\{\begin{array}{c} \varkappa \text{ ganz rational, mod. } m, \text{ prim zu } m \\ \alpha \neq 0 \text{ in } l \end{array}\right\}$$

fest. Man kann $\varkappa \equiv 1 \bmod. m$ normieren, indem man bei gegebenen ζ, S das Automorphieverhalten

$$\Theta^S = \Theta \cdot \zeta$$

fordert. Diese letztere Relation allein legt das Element Θ innerhalb aller Elemente $\neq 0$ aus L bis auf einen willkürlichen Faktor $\alpha \neq 0$ aus l als eine *bezüglich ζ, S normierte Kummersche Erzeugende von L/l* fest. Eine solche kann in bekannter Weise aus einer beliebigen Erzeugenden A von K/k nach der Methode der Lagrangeschen Resolvente konstruiert werden:

$$\Theta = \sum_{\mu \bmod. m} \zeta^{-\mu} \mathsf{A}^{iS^\mu},$$

wo der Exponent i nur so bestimmt ist, daß $\Theta \neq 0$ ausfällt, was stets für einen der Werte $i = 1, \ldots, m-1$ der Fall ist.

Anstatt durch *eine* Erzeugende Θ kann man L/l auch invariant durch die multiplikative Gruppe *aller* $\Theta \neq 0$ aus L charakterisieren, für die $\Theta^m = \omega$ in l liegt, oder auch durch die Gruppe der zugehörigen $\omega \neq 0$ aus l. Diese Gruppen sind zyklisch von der Ordnung m über der Gruppe der $\alpha \neq 0$ aus l bzw. der Gruppe der α^m, und die zuerst beschriebene Erzeugung läuft auf die Auswahl eines Basiselements Θ bzw. ω für sie hinaus.

Unsere Fragestellung kann dann folgendermaßen ausgesprochen werden: *Wie hängt diese Kummersche Erzeugung von L/l mit einer entsprechenden arithmetisch ausgezeichneten Erzeugung des Restklassenkörpers $\mathfrak{R}/\mathfrak{k}$ zusammen?*

Die Antwort auf diese Frage fällt naturgemäß ganz verschiedenartig aus, je nachdem welcher der beiden wesentlich zu unterscheidenden Fälle $(m, p) = 1$ oder $m = p^n$ für den Grad m von L/l in seinem Verhältnis zur Charakteristik p von $\mathfrak{k}$ vorliegt. Denn im ersteren Falle besitzt auch $\mathfrak{R}/\mathfrak{k}$ als arithmetisch ausgezeichnete Erzeugung eine solche vom Kummerschen Typus, im letzteren Falle dagegen tritt an deren Stelle eine Erzeugung vom Artin-Schreierschen Typus, in der Albert-Wittschen Verallgemeinerung auf den Grad p^n statt p.

Ich behandle zunächst kurz den trivialen Fall $(m, p) = 1$. Hier gehört ζ als über k unverzweigtes Element aus l bereits zu k, und seine Restklasse z ist eine primitive m-te Einheitswurzel in $\mathfrak{k}$; umgekehrt folgt übrigens aus dem Vorhandensein einer primitiven m-ten Einheitswurzel z in $\mathfrak{k}$ auch, daß der multiplikationstreue Repräsentant ζ von z in k eine primitive m-te Einheitswurzel ist. Ist nun dementsprechend

$$\mathfrak{R} = \mathfrak{k}(t) \quad \text{mit} \quad t^m = w, \quad w \text{ in } \mathfrak{k},$$
$$t^S = t \cdot z$$

eine bezüglich z, S normierte Kummersche Erzeugung von $\mathfrak{R}/\mathfrak{k}$, so liefert der Übergang zu den multiplikationstreuen Repräsentanten Θ, ω, ζ von t, w, z in K, k, k ersichtlich eine bezüglich ζ, S normierte Kummersche Erzeugung von K/k und damit auch von L/l. Allgemeiner entsteht die L in l zugeordnete Gruppe ω aus der $\mathfrak{R}$ in $\mathfrak{k}$ zugeordneten Gruppe w einfach, indem man zu den multiplikationstreuen Repräsentanten ω der w übergeht und noch mit beliebigen m-ten Potenzen α^m aus l multipliziert.

Ich komme nunmehr zum eigentlichen Ziel dieser Arbeit, der Behandlung des nicht-trivialen Falles $m = p^n$. Hier besitzt $\mathfrak{R}/\mathfrak{k}$ nach Witt eine arithmetisch ausgezeichnete Erzeugung von folgender Art:

$$\mathfrak{R} = \mathfrak{k}(x_n) \quad \text{mit} \quad x_n^p = x_n + c_n.$$

Dabei sind

$$\boldsymbol{c}_n = (c_0, \ldots, c_{n-1}), \qquad \boldsymbol{x}_n = (x_0, \ldots, x_{n-1})$$

n-gliedrige Vektoren aus $\mathfrak{k}$, $\mathfrak{R}$. Die Addition solcher Vektoren ist nicht etwa komponentenweise erklärt, sondern nach dem von Witt entwickelten besonderen Schema, die Potenzierung mit p dagegen komponentenweise. Die Vektoren $\boldsymbol{x}_n$, $\boldsymbol{c}_n$ liegen bis auf beliebige Substitutionen

$$\boldsymbol{x}_n \to \varkappa \boldsymbol{x}_n + \boldsymbol{a}_n, \qquad \boldsymbol{c}_n \to \varkappa \boldsymbol{c}_n + (\boldsymbol{a}_n^p - \boldsymbol{a}_n) \left\{ \begin{array}{c} \varkappa \text{ ganz rational, mod. } p^n, \text{ prim zu } p \\ \boldsymbol{a}_n \text{ } n\text{-gliedriger Vektor in } \mathfrak{k} \end{array} \right\}$$

fest. Man kann $\varkappa \equiv 1$ mod. p^n normieren, indem man bei gegebenem S das Automorphieverhalten

$$\boldsymbol{x}_n^S = \boldsymbol{x}_n + \boldsymbol{e}_n$$

fordert, wo

$$\boldsymbol{e}_n = (e, 0, \ldots, 0)$$

mit dem Einselement e von $\mathfrak{k}$ gebildet ist. Diese letztere Relation allein legt den Vektor $\boldsymbol{x}_n$ innerhalb aller n-gliedrigen Vektoren aus $\mathfrak{R}$ bis auf einen willkürlichen Summanden $\boldsymbol{a}_n$ aus $\mathfrak{k}$ als eine *bezüglich S normierte Wittsche Erzeugende von* $\mathfrak{R}/\mathfrak{k}$ fest.

Anstatt durch *einen* erzeugenden Vektor $\boldsymbol{x}_n$ kann man $\mathfrak{R}/\mathfrak{k}$ auch invariant durch die additive Gruppe *aller* n-gliedrigen Vektoren $\boldsymbol{x}_n$ aus $\mathfrak{R}$ charakterisieren, für die $\boldsymbol{x}_n^p - \boldsymbol{x}_n = \boldsymbol{c}_n$ in $\mathfrak{k}$ liegt, oder auch durch die Gruppe der zugehörigen Vektoren $\boldsymbol{c}_n$ aus $\mathfrak{k}$. Diese Gruppen sind zyklisch von der Ordnung p^n über der Gruppe der $\boldsymbol{a}_n$ aus $\mathfrak{k}$ bzw. der Gruppe der $\boldsymbol{a}_n^p - \boldsymbol{a}_n$, und die zuerst beschriebene Erzeugung läuft auf die Auswahl eines Basiselements $\boldsymbol{x}_n$ bzw. $\boldsymbol{c}_n$ für sie hinaus.

Aus einem Grunde, der mit der am Schluß von **1** gemachten Bemerkung zusammenhängt — ich komme darauf unten in Fußnoten 4, 5 zurück —, ist es für unseren Zweck notwendig, diese Wittsche Erzeugung von $\mathfrak{R}/\mathfrak{k}$ noch dadurch zu überbauen, daß man den obigen n-gliedrigen Vektor $\boldsymbol{c}_n$ aus $\mathfrak{k}$ beliebig zu einem abzählbar unendlichen Vektor

$$\boldsymbol{c} = (c_0, \ldots, c_{n-1}, c_n, \ldots)$$

aus $\mathfrak{k}$ auffüllt, sodaß also $\boldsymbol{c}_n$ als der n-te Abschnitt von $\boldsymbol{c}$ erscheint. Durch

$$\overline{\mathfrak{R}} = \mathfrak{k}(\boldsymbol{x}) \quad \text{mit} \quad \boldsymbol{x}^p = \boldsymbol{x} + \boldsymbol{c}$$

wird dann ein Turm (d. h. eine Körperfolge, in der jeder Körper die vorhergehenden enthält) über $\mathfrak{k}$ zyklischer Körper der Grade $p, p^2, \ldots$ definiert. Der abzählbar unendliche Vektor

$$\boldsymbol{x} = (x_0, \ldots, x_{n-1}, x_n, \ldots)$$

kann dabei zunächst so gewählt werden, daß sein n-ter Abschnitt der obige n-gliedrige Vektor $\boldsymbol{x}_n$ ist; daher ist der n-te Abschnitt des Turmes $\overline{\mathfrak{R}}$ der obige Körper $\mathfrak{R}$. Bezeichnet ferner S eine Fortsetzung des obigen Automorphismus S von $\mathfrak{R}/\mathfrak{k}$ auf $\overline{\mathfrak{R}}/\mathfrak{k}$, so können die weiteren Komponenten von $\boldsymbol{x}$ noch so normiert werden, daß

$$\boldsymbol{x}^S = \boldsymbol{x} + \boldsymbol{e}$$

gilt, wo

$$\boldsymbol{e} = (e, 0, \ldots)$$

ist, daß also $\boldsymbol{x}$ eine bezüglich S normierte Wittsche Erzeugende von $\overline{\mathfrak{R}}/\mathfrak{k}$ ist.

Invariant ist $\overline{\mathfrak{R}}/\mathfrak{k}$ charakterisiert durch die Gruppe aller abzählbar unendlichen Vektoren $\boldsymbol{x}$ aus $\overline{\mathfrak{R}}$, für die $\boldsymbol{x}^p - \boldsymbol{x} = \boldsymbol{c}$ in $\mathfrak{k}$ liegt, oder auch durch die Gruppe der zuge-

hörigen Vektoren $\boldsymbol{c}$ aus $\mathfrak{k}$. Durch Bildung der n-ten Abschnitte entstehen aus diesen Gruppen $\boldsymbol{x}, \boldsymbol{c}$ die obigen $\mathfrak{R}/\mathfrak{k}$ invariant charakterisierenden Gruppen $\boldsymbol{x}_n, \boldsymbol{c}_n$[4]).

Dem Turm $\overline{\mathfrak{R}}/\mathfrak{k}$ mit n-tem Abschnitt $\mathfrak{R}$ entsprechen nach der Strukturtheorie umkehrbar eindeutig Türme $\overline{K}/k$ und $\overline{L}/l$ von gleicher Struktur, deren n-te Abschnitte die obigen Körper K und L sind. Den Vektoren

$$\boldsymbol{x} = (x_\nu) \quad \text{aus} \quad \overline{\mathfrak{R}},$$
$$\boldsymbol{c} = (c_\nu) \quad \text{aus} \quad \mathfrak{k}$$

entsprechen ferner umkehrbar eindeutig die Elemente

$$\xi = \sum_{\nu=0}^{\infty} \xi_\nu p^\nu \quad \text{aus} \quad \overline{K},$$

$$\gamma = \sum_{\nu=0}^{\infty} \gamma_\nu p^\nu \quad \text{aus} \quad k$$

nach dem Teichmüller-Wittschen Schema:

$$\xi_\nu = \text{multiplikationstreuer Repräsentant von } x_\nu^{p^{-\nu}} \text{ in } \overline{K}$$
$$\gamma_\nu = \quad " \quad " \quad " \quad c_\nu^{p^{-\nu}} \text{ in } k,$$

und ebenso dem Vektor $\boldsymbol{e} = (e, 0, \ldots)$ aus $\mathfrak{k}$ das Einselement 1 aus k. Den Relationen

$$\boldsymbol{x}^p = \boldsymbol{x} + \boldsymbol{c}, \quad \boldsymbol{x}^S = \boldsymbol{x} + \boldsymbol{e}$$

in $\overline{\mathfrak{R}}$ entsprechen die Relationen

$$\xi^P = \xi + \gamma, \quad \xi^S = \xi + 1$$

in $\overline{K}$. Dabei ist P der (schon in **1** eingeführte) Automorphismus von $\overline{K}/k_0$ mit der Wirkung

$$\xi^P = \sum_{\nu=0}^{\infty} \xi_\nu^p p^\nu,$$

entstehend durch Übertragung des Automorphismus $\overline{\mathfrak{R}} \to \overline{\mathfrak{R}}^p$ von $\overline{\mathfrak{R}}/\mathfrak{k}_0$ auf $\overline{K}/k_0$ nach dem eingangs besprochenen Schema; S entsteht nach dem gleichen Schema durch Übertragung des Automorphismus S von $\overline{\mathfrak{R}}/\mathfrak{k}$ auf $\overline{K}/k$ und ist eine Fortsetzung des Automorphismus S von K/k.

Nun ist ζ eine Einseinheit aus l und ξ ein ganzes Element aus $\overline{K}$. Daher können wir im Sinne des in **1** eingeführten erweiterten Potenzbegriffs die Potenzen

$$\Theta = \zeta^\xi, \qquad \omega = \zeta^{p^n \xi}$$

bilden; an Stelle der Körper $\mathfrak{k}, k, l$ in **1** sind hier die Körper $\overline{\mathfrak{R}}$, $\overline{K}$, $\overline{L}$ zugrunde zu legen, so daß also die Elemente Θ, ω jedenfalls in $\overline{L}$ liegen. Nach den Potenzregeln (2), (3) hat man

$$\Theta^S = \zeta^{\xi S} = \zeta^{\xi+1} = \zeta^\xi \cdot \zeta = \Theta \cdot \zeta \text{ [5])},$$
$$\Theta^{p^n} = (\zeta^\xi)^{p^n} = \zeta^{p^n \xi} = \omega .$$

---

[4]) Es sei ausdrücklich bemerkt, daß der speziellen Auffüllung von $\boldsymbol{c}_n$ zu $\boldsymbol{c}$ durch lauter Nullen keineswegs die entsprechende spezielle Auffüllung von $\boldsymbol{x}_n$ zu $\boldsymbol{x}$ entspricht.

[5]) Würde man nur mit den n-gliedrigen Vektoren $\boldsymbol{x}_n$, $\boldsymbol{c}_n$, $\boldsymbol{e}_n$ arbeiten, so hätte man nur

$$\xi^P \equiv \xi + 1 \bmod p^n.$$

und daraus kann nicht auf

$$\zeta^{\xi^P} = \zeta^{\xi+1}$$

geschlossen werden, ebenso wie $\zeta^{p^n \xi}$ nach dem Ergebnis des Textes sicher nicht gleich 1 ist, obwohl $\zeta^{p^n} = 1$ ist. Die Potenzregel (3) bleibt eben bei Vertauschung der Rollen von a und α nicht allgemein gültig.

Hiernach liegt ω in l, also Θ in L, und es ist

$$L = l(\Theta),$$

d. h. Θ ist eine bezüglich ζ, S normierte Kummersche Erzeugung von L/l [6]).

Allgemeiner entnimmt man aus den vorstehenden Ausführungen ohne weiteres:

Die L invariant zugeordneten Gruppen Θ in L und ω in l entstehen in der Form

$$\Theta = \zeta^{\xi}\alpha, \quad \omega = \zeta^{p^n\xi}\,\alpha^{p^n} \qquad (\alpha \neq 0 \text{ in } l),$$

wo ξ die additive Gruppe aller ganzen Elemente aus $\bar{K}$ durchläuft, für die

$$\xi^P = \xi + \gamma$$

mit ganzem γ aus k ist.

Damit ist der Mechanismus aufgedeckt, nach dem die Kummersche Erzeugung von L/l mit der Wittschen Erzeugung von $\mathfrak{R}/\mathfrak{k}$ zusammenhängt.

3.

Ich gehe noch kurz auf den für die Anwendung auf algebraische Zahlkörper in Frage kommenden Spezialfall ein, daß k ein endlicher Körper von $q = p^f$ Elementen ist. Dann gibt es nur einen einzigen Turm $\bar{\mathfrak{R}}$ über $\mathfrak{k}$ zyklischer Körper der Grade $p, p^2, \ldots$, und dementsprechend auch nur je einen einzigen Turm $\bar{K}$ bzw. $\bar{L}$ über k bzw. l zyklischer Körper der Grade $p, p^2, \ldots$. Für $\bar{\mathfrak{R}}$ und $\bar{K}$ kann dabei $S = Q = P^f$ gesetzt werden (Artin-Automorphismus).

Die L zugeordnete Gruppe ω in l ist dann die Gruppe *aller* $\omega \neq 0$ aus l, für die $l(\sqrt[p^n]{\omega})$ unverzweigt über l ist, also die Gruppe der *p^n-primären* Elemente aus l. Der zuletzt ausgesprochene Satz gibt also eine explizite Bestimmung dieser Gruppe, und zwar mit Hinblick auf die Potenzregel (1) in Form einer Kongruenzcharakterisierung.

Überdies ergibt sich eine explizite Bestimmung des zugehörigen *Artin-Symbols* $\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n}$. Dieses ist definiert durch

$$\Theta^Q = \Theta \cdot \left(\frac{\omega}{\mathfrak{p}}\right)_{p^n}, \quad \text{wo } \Theta^{p^n} = \omega.$$

Führt man die gewonnene Potenzdarstellung

$$\Theta = \zeta^{\xi}\alpha \qquad (\alpha \neq 0 \text{ in } l)$$

mit

$$\xi^P = \xi + \gamma, \quad \gamma \text{ ganz in } k,$$

ein, so hat man

$$\xi^Q = \xi^{P^f} = \xi + \gamma + \gamma^P + \cdots + \gamma^{P^{f-1}} = \xi + \mathrm{Sp}\,\gamma,$$

also

$$\Theta^Q = \zeta^{\xi^Q}\alpha = \zeta^{\xi}\alpha \cdot \zeta^{\mathrm{Sp}\,\gamma} = \Theta \cdot \zeta^{\mathrm{Sp}\,\gamma},$$

d. h.

$$\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n} = \zeta^{\mathrm{Sp}\,\gamma}.$$

---

[6]) Den Hinweis auf diese einfache Schlußführung an Stelle meines ursprünglichen komplizierteren Beweises verdanke ich E. Witt.

Wir haben also:

Ist

$$\omega = \zeta^{p^n \xi} \alpha^{p^n} \qquad \begin{Bmatrix} \xi \text{ ganz in } \overline{K} \\ \alpha \neq 0 \text{ in } l \end{Bmatrix}$$

eine p^n-primäre Zahl aus l und dabei

$$\xi^P = \xi + \gamma,$$

so ist das zugehörige Artin-Symbol durch

$$\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n} = \zeta^{S\mathfrak{p}\,\gamma}$$

gegeben.

Faßt man l als $\mathfrak{p}$-adische Erweiterung eines die p^n-ten Einheitswurzeln enthaltenden algebraischen Zahlkörpers Λ für einen Primteiler $\mathfrak{p}$ von p auf, so hat man eine Kongruenzcharakterisierung der für $\mathfrak{p}$ p^n-primären ω aus Λ und eine darauf gegründete explizite Bestimmung des Artin-Symbols $\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n}$ in Λ.

Eingegangen 7. Mai 1936.

Über die Ausnahmeklassen bei abstrakten hyperelliptischen Funktionenkörpern.

Von *Helmut Hasse* und *Hermann Ludwig Schmid* in Göttingen.

K sei ein algebraischer Funktionenkörper einer Unbestimmten vom Geschlecht g über einem algebraisch abgeschlossenen Konstantenkörper k der Charakteristik p (gleich 0 oder Primzahl). Eine Divisorenklasse C_g von K vom Grade g heißt Ausnahmeklasse, wenn $\dim C_g > 1$ ist. Die Kenntnis der Ausnahmeklassen ist für eine umkehrbar eindeutige Beschreibung der Divisorenklassen nullten Grades wünschenswert.

Wir geben in dieser Note für den Fall eines hyperelliptischen Funktionenkörpers K eine genaue Charakterisierung der Ausnahmeklassen. Dies gelingt hier, weil der rationale Funktionenkörper $k(x)$ innerhalb K als Quotientenkörper der ganzen Differentiale invariant gekennzeichnet ist. Auf Grund der Kenntnis der Ausnahmeklassen ist es dann leicht, eine eindeutige Repräsentation der Divisorenklassen nullten Grades zu geben, wie dies z. B. bei elliptischen Körpern durch die Quotienten $\frac{\mathfrak{P}}{\mathfrak{Q}}$ geschieht, wo $\mathfrak{Q}$ ein fester und $\mathfrak{P}$ ein variabler Primdivisor ist. Die vorbereitenden Ausführungen über eine Erzeugung und die ganzen Differentiale von K sind eine direkte Verallgemeinerung der entsprechenden von Hasse aufgestellten Sätze für den Fall eines elliptischen Funktionenkörpers, der in unseren Ausführungen unter dem allgemeinen Begriff des hyperelliptischen Funktionenkörpers subsumiert werden kann [1]). Zum Schluß geben wir eine elementare Bestimmung der Anzahl der Divisorenklassen C_0 von K mit $C_0^2 = 1$.

1. Wenn K nicht rational ist ($g \geqq 1$), so folgt nach dem Riemann-Rochschen Satz für eine Klasse C_2 vom Grade 2

$$\dim C_2 = 0, 1 \text{ oder } 2.$$

K ist dann und nur dann hyperelliptisch, wenn mindestens eine Klasse C_2 mit $\dim C_2 = 2$ existiert. Dies ist gleichbedeutend damit, daß K quadratisch erzeugbar ist.

Denn seien $\mathfrak{A}$, $\mathfrak{B}$ zwei linear unabhängige ganze Divisoren aus einer Klasse C_2 mit $\dim C_2 = 2$ und

$$z \cong \frac{\mathfrak{A}}{\mathfrak{B}}.$$

Da K nicht rational ist (sonst wäre $\dim C_2 = 3$), folgt $(\mathfrak{A}, \mathfrak{B}) = 1$, also $[K : k(z)] = 2$.

Sei umgekehrt K nicht rational und quadratisch erzeugbar, $[K : k(z)] = 2$. Da in $k(z)$ alle Primdivisoren äquivalent sind, bilden diese eine einzige Klasse auch in K; deren Grad und Dimension ist gleich 2.

---

[1]) H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper II, Journ. f. Math. **175** (1936).

Nach der Geschlechtsformel

$$g = \frac{d_z}{2} - (n_z - 1)$$

ist dann

$$d_z = 2g + 1 \geqq 3.$$

Also ist mindestens ein Verzweigungspunkt $\mathfrak{O}$ für $K/k(z)$ vorhanden. Daraus resultiert folgende Erzeugung von K:

Es gibt in K ein Element x mit dem genauen Nenner $\mathfrak{O}^2$. Wegen

$$\dim \mathfrak{O}^{2g+1} - \dim \mathfrak{O}^{2g} = 1$$

existiert ein Element y aus K mit dem genauen Nenner $\mathfrak{O}^{2g+1}$. Dann bilden für jedes $n \geqq 0$ die Potenzprodukte

$$x^i y^j \quad \text{mit} \quad 0 \leqq i, \quad 0 \leqq j \leqq 1, \quad 2i + (2g+1)\, j \leqq n$$

eine Basis der ganzen Multipla von $\frac{1}{\mathfrak{O}^n}$ in K. Insbesondere stellen die Elemente

$$1, x, \ldots, x^{2g+1}; \quad y, xy, \ldots, x^g y$$

eine Basis der ganzen Multipla von $\frac{1}{\mathfrak{O}^{4g+2}}$ in K dar. Also muß y^2 (mit dem genauen Nenner $\mathfrak{O}^{4g+2}$) sich durch diese linear darstellen lassen:

$$F(x, y) = y^2 + f_g(x)\, y + f_{2g+1}(x) = 0. \tag{1}$$

$F(x, y)$ ist in x bzw. y vom Grade $2g + 1$ bzw. 2. $f_g(x)$ ist ein Polynom in x höchstens vom Grade g, $f_{2g+1}(x)$ ein Polynom in x vom genauen Grade $2g + 1$. $K/k(x)$ ist vom Grade 2 und separabel.

Der Integritätsbereich $J_{\mathfrak{O}}$ der höchstens für $\mathfrak{O}$ gebrochenen Elemente aus K fällt mit dem Integritätsbereich J_x der in bezug auf $k[x]$ ganz algebraischen Elemente aus K zusammen und hat über $k[x]$ die Basis $1, y$:

$$J_{\mathfrak{O}} = k[x, y] = k[x] + k[x]\, y = J_x.$$

2. Wir legen im folgenden für K die Erzeugung (1) zugrunde. Dann beweisen wir den

Satz 1.

$$du = \frac{dx}{F_y(x, y)} \cong \mathfrak{O}^{2g-2} \tag{2}$$

ist ein ganzes Differential von K. $(1, x, \ldots, x^{g-1})\, du$ ist ein System von g linear unabhängigen ganzen Differentialen von K. Das allgemeine ganze Differential von K hat die Form

$$\varphi(x)\, du, \tag{2a}$$

wo $\varphi(x)$ ein Polynom höchstens vom Grade $g - 1$ ist.

Beweis. Es ist

$$F_y(x, y) \cong y - y',$$

wo y' die zu y konjugierte über $k(x)$ bezeichnet. Es kommt also auf den Nachweis der Divisorengleichung

$$dx \cong \mathfrak{O}^{2g-2}\, (y - y')$$

an. Wegen $dx \cong \frac{\mathfrak{D}_x}{\mathfrak{O}^4}$ ($\mathfrak{D}_x$ Differentendivisor für $K/k(x)$) ist

$$\mathfrak{D}_x \cong \mathfrak{O}^{2g+2}\, (y - y') \tag{3}$$

zu zeigen. Wegen $J_x = J_{\mathfrak{O}}$ stimmt für jedes $\mathfrak{P} \neq \mathfrak{O}$ der Beitrag zu $\mathfrak{D}_x$ mit dem Beitrag von $y - y'$ überein. Es bleibt also die Äquivalenz (3) nur noch für $\mathfrak{O}$ zu zeigen. Nun ist $\frac{x^g}{y}$ Primelement für $\mathfrak{O}$. Der $\mathfrak{O}$-Beitrag zu $\mathfrak{D}_x$ ist daher gleich dem $\mathfrak{O}$-Beitrag zur Elementdifferente

$$\frac{x^g}{y} - \frac{x^g}{y'} \cong \mathfrak{O}^{2g+2}(y - y').$$

Damit ist Satz 1 bewiesen.

Bemerkung. Ist $g = 1$ (K elliptisch), so ist weder $k(x)$ noch eine Klasse C_2 mit $\dim C_2 = 2$ eindeutig bestimmt. Vielmehr existieren unendlich viele Körper $k(x)$, über denen K quadratisch erzeugbar ist, und jede Klasse C_2 hat die Dimension 2 [1]). Ist dagegen $g > 1$ (K echt hyperelliptisch), so ist nach Satz 1 $k(x)$ innerhalb K als Quotientenkörper der ganzen Differentiale von K invariant charakterisiert. Aus den folgenden Ausführungen (Satz 2) sieht man leicht, daß nur eine Klasse C_2 mit $\dim C_2 = 2$ vorhanden ist, nämlich die Klasse der Primdivisoren von $k(x)$.

Im folgenden bezeichnen kleine deutsche Buchstaben immer Divisoren aus $k(x)$. Es sei $\mathfrak{o} = \mathfrak{O}^2$. Wegen (2) hat das allgemeine ganze Differential (2a) von K die Divisorendarstellung

$$\varphi(x)\, du \cong \frac{\mathfrak{g}}{\mathfrak{o}^\nu}\, \mathfrak{O}^{2g-2} = \mathfrak{G}\mathfrak{G}'\mathfrak{O}^{2g-2-2\nu} = \mathfrak{G}\mathfrak{O}^{g-1-\nu}(\mathfrak{G}\mathfrak{O}^{g-1-\nu})' \quad (0 \leqq \nu \leqq g-1).$$

(Der Strich soll stets die Konjugiertenbildung bezüglich $k(x)$ andeuten.) Wir haben daher:

Satz 2. *Die ganzen Divisoren aus der Differentialklasse W von K sind genau die Normen bezüglich $k(x)$ der ganzen Divisoren vom Grade $g-1$ von K.*

3. Wir nennen einen ganzen Divisor von K *primitiv*, wenn er durch keinen Divisor von $k(x)$ teilbar ist. Jeder ganze Divisor $\mathfrak{G}$ von K vom Grade g besitzt eine eindeutige Produktdarstellung

$$\mathfrak{G} = (\mathfrak{D}\mathfrak{D}')\,\mathfrak{R} = \mathfrak{d}\mathfrak{R},$$

wo $\mathfrak{D}$ vom Grade n in K ($\mathfrak{d}$ also vom Grade n in $k(x)$) und $\mathfrak{R}$ primitiv ist. Wir nennen n den *Imprimitivitätsgrad* von $\mathfrak{G}$.

Satz 3. *Ist G die Klasse des ganzen Divisors $\mathfrak{G}$ vom Grade g, so ist die Dimension der Ergänzungsklasse $\frac{W}{G}$ gleich dem Imprimitivitätsgrad n von $\mathfrak{G}$ oder also*

$$\dim G = 1 + n.$$

Der Imprimitivitätsgrad von $\mathfrak{G}$ ist somit eine Eigenschaft der zugehörigen Klasse.

Beweis. Die durch $\mathfrak{G}$ teilbaren ganzen Differentiale müssen nach Satz 2 sogar durch $\mathfrak{D}\mathfrak{D}'\mathfrak{R}\mathfrak{R}'$ teilbar sein. Der komplementäre Teiler muß dann von der Form $\mathfrak{f} = \mathfrak{S}\mathfrak{S}'$ ($\mathfrak{S}$ vom Grade $n-1$) sein und kann innerhalb dieser Form beliebig gewählt werden. Es gibt aber genau n linear unabhängige ganze Divisoren $\mathfrak{f}$ vom Grade $n-1$ von $k(x)$. Also ist $\dim \frac{W}{G} = n$, w. z. b. w.

Aus Satz 3 ergibt sich sofort der

Satz 4. *Ein System von g Primdivisoren $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ist dann und nur dann nicht speziell, d. h. dim $(\mathfrak{P}_1 \cdots \mathfrak{P}_g) = 1$, wenn der Imprimitivitätsgrad des Divisors $\mathfrak{P}_1 \cdots \mathfrak{P}_g$ gleich Null ist, wenn also $\mathfrak{P}_1 \cdots \mathfrak{P}_g$ durch keinen Divisor aus $k(x)$ teilbar ist.*

Wir können den Inhalt von Satz 4 auch so wenden, daß die Charakterisierung der Ausnahmeklassen formuliert wird:

Satz 4a. *Eine Klasse C_g vom Grade g ist dann und nur dann Ausnahmeklasse, wenn ihr Imprimitivitätsgrad positiv ist.*

4. Wir geben jetzt die eineindeutige Beschreibung der Divisorenklassen nullten Grades von K.

Satz 5. *Die Divisorenklassen nullten Grades von K werden umkehrbar eindeutig repräsentiert durch die Quotienten*

$$\frac{\mathfrak{P}_1 \cdots \mathfrak{P}_\nu}{\mathfrak{O}^\nu} \qquad (0 \leqq \nu \leqq g),$$

wobei $\mathfrak{P}_1 \cdots \mathfrak{P}_\nu$ alle primitiven, zu $\mathfrak{O}$ primen Divisoren ν-ten Grades von K durchläuft.

Beweis. Den Klassen nullten Grades C_0 entsprechen umkehrbar eindeutig Klassen g-ten Grades C_g durch die Beziehung

$$C_0(\mathfrak{O}^g) = C_g.$$

Es genügt also, eine eineindeutige Repräsentation der Klassen C_g anzugeben. Sind nun $\mathfrak{G}$ und $\mathfrak{H}$ zwei ganze Divisoren aus einer Klasse C_g und

$$\begin{aligned} \mathfrak{G} &= \mathfrak{g}\mathfrak{G}_0 \\ \mathfrak{H} &= \mathfrak{h}\mathfrak{H}_0 \end{aligned} \qquad (\mathfrak{g}, \mathfrak{h} \text{ ganz in } k(x), \quad \mathfrak{G}_0 \text{ und } \mathfrak{H}_0 \text{ primitiv})$$

ihre eindeutigen Zerlegungen, so folgt, da nach Satz 3 der Grad von $\mathfrak{g}$ gleich dem Grad von $\mathfrak{h}$ ist, $\mathfrak{G}_0 \sim \mathfrak{H}_0$ und daraus (nach evtl. Ergänzung der Divisoren $\mathfrak{G}$ und $\mathfrak{H}$ auf den Grad g) wegen der Primitivität $\mathfrak{G}_0 = \mathfrak{H}_0$. Ersetzen wir noch $\mathfrak{g}$ durch den ihm äquivalenten Divisor $\mathfrak{O}^{2n}$ (n Imprimitivitätsgrad von C_g), so haben wir aus C_g eindeutig einen ganzen Divisor

$$\mathfrak{O}^{2n}\mathfrak{G}_0$$

bestimmt. Ein etwa in $\mathfrak{G}_0$ noch vorkommender Faktor $\mathfrak{O}^1$ kann zur Potenz $\mathfrak{O}^{2n}$ dazu genommen werden. Daraus folgt jetzt unmittelbar die Gültigkeit von Satz 5.

5. Eine hübsche Anwendung von Satz 5 ist die Bestimmung der Anzahl der Klassen C_0 mit $C_0^2 = 1$. Es sind dies genau die Klassen, für die $C_0 = C_0'$ ist. Nach Satz 5 soll also

$$(4) \qquad \frac{\mathfrak{P}_1 \cdots \mathfrak{P}_\nu}{\mathfrak{O}^\nu} = \frac{\mathfrak{P}_1' \cdots \mathfrak{P}_\nu'}{\mathfrak{O}^\nu} \qquad (\mathfrak{P}_1 \cdots \mathfrak{P}_\nu \text{ primitiv}, \ 0 \leqq \nu \leqq g)$$

sein. Dies ist aber nur für $\mathfrak{P}_i = \mathfrak{P}_i'$ $(i = 1, \ldots, \nu)$ möglich. Die in (4) zur Repräsentation unserer gesuchten Klassen benutzten $\mathfrak{P}$ können also nur die von $\mathfrak{O}$ verschiedenen Verzweigungspunkte sein. Ist N die Anzahl aller Verzweigungspunkte von K, so ist unsere gesuchte Anzahl gleich

$$\sum_{i=0}^{N-1} \binom{N-1}{i} = 2^{N-1} \quad \text{für } N-1 \leqq g$$

und

$$\sum_{i=1}^{g} \binom{N-1}{i} \qquad \text{für } N-1 > g.$$

Ist die Charakteristik $p \neq 2$, so ist $N = 2g + 2$ und $\sum_{i=0}^{g} \binom{N-1}{i} = 2^{2g}$. Für $p = 2$

ist in (1) notwendig $f_g(x) \neq 0$. Wegen $\mathfrak{D}_x \cong \mathfrak{D}^{2g+2} f_g(x)$ ist N eine der Zahlen von 1 bis $g+1$.

Wir fassen unser Ergebnis zusammen in

Satz 6. *Die Anzahl der Klassen C_0 mit $C_0^2 = 1$ ist für $p \neq 2$ gleich 2^{2g}, für $p = 2$ dagegen gleich 2^{N-1}, wo N als Anzahl der Verzweigungspunkte von K eine der Zahlen 1 bis $g+1$ ist.*

Der erste Teil der Aussage des Satzes 6 ist ein Teilresultat des Desideratums: Die Anzahl der Klassen C_0 mit $C_0^n = 1$ ist für $(n, p) = 1$ gleich n^{2g}.

Den zweiten Teil vergleichen wir mit bekannten Resultaten einer früher erschienenen Arbeit [2]). Dort wurde festgestellt, daß die Anzahl der Klassen C_0 mit $C_0^p = 1$ gleich p^γ ist, wo γ als Rang einer gewissen invarianten Matrix M von K eine der Zahlen 0 bis g ist [3]). Der Vergleich beider Resultate ergibt den

Satz 7. *Ist die Charakteristik $p = 2$, so ist der Rang γ der Matrix M gleich $N-1$, wo N die Anzahl der Verzweigungspunkte von K ist.*

---

[2]) H. Hasse und E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p, Monatshefte f. Math. u. Phys. **43** (1936).

[3]) Ist $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ein nicht spezielles System von lauter verschiedenen Primdivisoren und $\pi_1, \ldots, \pi_g$ ein zugehöriges System lokaler Primelemente, so existiert in K ein System $v_1, \ldots, v_g$ von Elementen, die ganze Multipla von $\dfrac{1}{(\mathfrak{P}_1 \cdots \mathfrak{P}_g)^p}$ sind und die Entwicklungen

$$v_j = \frac{e_{ij}}{\pi_i^p} - \frac{a_{ij}}{\pi_i} + \cdots$$

besitzen. Dann ist γ der Rang der Matrix $M = AA^p \cdots A^{p^{g-1}}$, wo $A = (a_{ij})$ ist.

Eingegangen 25. August 1936.